#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	:	
Kunio Kobayashi et al.	:	
Serial No.: To be assigned	:	Art Unit: To be assigned
Filed: Herewith	:	Examiner: To be assigned
For: SYSTEM AND METHOD FOR QUANTITATIVE COMPETITION AND RECORDING MEDIUM HAVING RECORDED THEREON PROGRAM FOR IMPLEMENTING THEM	:	Atty Docket: 0162/00561

SUBMISSION OF CERTIFIED PRIORITY DOCUMENT(S) and CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Commissioner for Patents
Washington, D.C. 20231

Sir:

Priority under 35 U.S.C. § 119 is hereby claimed to the following priority document(s), certified copies of which are enclosed. The documents were filed in a foreign country within the proper statutory period prior to the filing of the above-referenced United States patent application.

Priority Document Serial No.	Country	Filing Date
205004/99	Japan	July 19,1999
247060/99	Japan	September 1,1999
2000-016020	Japan	January 25, 2000
2000-047323	Japan	February 24, 2000

Acknowledgement of this claim and submission in the next official communication is respectfully requested.

Respectfully submitted,

Morris Liss

Morris Liss, Reg. No. 24,510
Pollock, Vande Sande & Amernick
1990 M Street, N.W.
Washington, D.C. 20036-3425
Telephone: 202-331-7111

Date: July 19, 2000

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:　１９９９年　７月１９日

出願番号
Application Number:　平成１１年特許願第２０５００４号

出願人
Applicant (s):　日本電信電話株式会社

２０００年　６月２３日

特許庁長官
Commissioner,
Patent Office　近藤隆彦

出証番号　出証特２０００－３０４６８３５

【書類名】　特許願
【整理番号】　NTTH115596
【提出日】　平成11年 7月19日
【あて先】　特許庁長官殿
【国際特許分類】　G09C
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小林　邦生
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　森田　光
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100066153
　【弁理士】
　【氏名又は名称】　草野　卓
【選任した代理人】
　【識別番号】　100100642
　【弁理士】
　【氏名又は名称】　稲垣　稔
【手数料の表示】
　【予納台帳番号】　002897
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子競争入札方法、その装置及びプログラム記録媒体

【特許請求の範囲】

【請求項１】　複数の入札装置から、入札価格と、その入札装置を特定する識別子とを開札装置へ送り、開札装置で受信した入札価格中の最大値又は最小値を落札価格とし、その落札価格とその入札価格を提示した入札装置の識別子を出力する電子競争入札方法において、

入札装置は入札価格を一方向性関数を用いて整数の入札指標に変換して、開札装置へ送り、

開札装置は各受信した入札指標から、非落札価格を全入札装置に知られることなく、最大入札価格又は最小入札価格を落札価格として決定することを特徴とする電子競争入札方法。

【請求項２】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）の上記入札指標を

$$\gamma_i = g\left(h^{f(PRi)}\left(IV_i\right)\right)$$

とし、ｇは一方向性関数を、IV_i は入札装置ｉに固有の初期値、ｆ（PR_i）は入札装置ｉの入札価格PR_i の関数であり、PR_i が大きくなる程大きな正の整数値を出力する関数である、$h^{f(PRi)}$はIV_i に対して一方向性関数ｈをｆ（PR_i）回繰返すことを示し、

各入札装置ｉは$C_i = h^{f(n+1)}\left(IV_i\right)$（ｎは入札価格の上限値）を共有記録媒体に記録して全入札装置に公開していることを特徴とする請求項１記載の電子競争入札方法。

【請求項３】　開札装置での落札価格の決定は、

処理パラメータｋを上限値ｎに設定する過程と、

$\delta_i = g\left(h^{f(k)}\left(IV_i\right)\right)$ を各IV_i について演算するδ_i 演算過程と、

δ_i が入札指標γ_i と一致するか調べる照合過程と、

上記照合過程で何れのIV_i についても一致するものがなければ上記ｋを－１して上記δ_i 演算過程に戻る過程と、

上記照合過程で一致すると、その時のｋを落札価格とし、その一致したγ_i と

対応する識別子$ＩＤ_i$とを出力する過程とにより行われることを特徴とする請求項２記載の電子競争入札方法。

【請求項４】　開札装置に受信した各入札価格$ＰＲ_i$と識別子$ＩＤ_i$を、何れの装置からも参照可能な共有記録媒体に記録し、

上記落札価格ｋと識別子$ＩＤ_i$とに対する$h^{f(k)}（ＩＶ_i）$をも出力することを特徴とする請求項３記載の電子競争入札方法。

【請求項５】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）の上記入札指標を、

$$\gamma_i = g（h^{f(n,PRi)}（ＩＶ_i））$$

とし、ｇは一方向性関数、$ＩＶ_i$は入札装置ｉに固有の初期値、$ＰＲ_i$は入札装置ｉの入札価格、ｎは入札価格の上限値、ｆ（ｎ，$ＰＲ_i$）は$ＰＲ_i$が大きくなる程、小さな正の整数値を出力する関数、$h^{f(n,PRi)}$は$ＩＶ_i$に対して一方向性関数ｈをｆ（ｎ，$ＰＲ_i$）回繰返すことを示し、

各入札装置ｉは$Ｃ_i = h^{f(n,q-1)}（ＩＶ_i）$（ｑは入札価格の下限値）を共有記録媒体に記録して全入札装置に公開していることを特徴とする請求項１記載の電子競争入札方法。

【請求項６】　開札装置での落札価格の決定は、

処理パラメータｋを下限値ｑに設定する過程と、

$\delta_i = g（h^{f(n,k)}（ＩＶ_i））$を各$ＩＶ_i$について演算する$\delta_i$演算過程と

δ_iが入札指標γ_iと一致するか調べる照合過程と、

上記照合過程で何れの$ＩＶ_i$についても一致するものがなければ上記ｋを＋１して上記δ_i演算過程に戻る過程と、

上記照合過程で一致すると、その時のｋを落札価格とし、その一致したγ_iと対応する識別子$ＩＤ_i$とを出力する過程とにより行われることを特徴とする請求項５記載の電子競争入札方法。

【請求項７】　開札装置に受信した各入札価格$ＰＲ_i$と識別子$ＩＤ_i$を、何れの装置かも参照可能な共有記録媒体に記録し、

上記落札価格ｋと識別子$ＩＤ_i$と対応する$h^{f(n,k)}（ＩＶ_i）$をも出力するこ

とを特徴とする請求項６記載の電子競争入札方法。

【請求項８】　開札装置に入力された複数の入札指標γ_i、識別子ID_iを共有記録媒体に蓄積する過程と、

パラメータｋとｎをセットする過程と、

全入札装置ｉに$h^{f(k)}(IV_i)$の提示を要求する提示要求過程と、

その提示要求を受けた入札装置ｉはその初期値IV_iを用いて$h^{f(k)}(IV_i)$（$=D_i$）を生成して開札装置に入力する過程と、

開札装置は入力された全D_iを共有記録媒体に蓄積する過程と、

全D_iに対して、$h^{f(n+1)-f(k)}(D_i)$を作成する過程と、

これら$h^{f(n+1)-f(k)}(D_i)$が共有記録媒体上の対応するC_iと各々一致するかを検証する過程と、

その検証で全て一致すると、$g(D_i)$を生成する過程と、

その各$g(D_i)$が共有記録媒体上の入札指標γ_iに一致するかを検証する過程と、

その検証でγ_iと一致するものが１つもなければ、共有記録媒体上のC_iをD_iで上書き（$C_i \leftarrow D_i$）し、ｋを－１して上記提示要求過程に戻る過程と、

上記検証でγ_iと一致するものがあればその時のｋを落札価格とし、そのｋと、この落札価格を提示した入札装置の識別子ID_iを出力する過程と

を有することを特徴とする請求項２記載の電子競争入札方法。

【請求項９】　開札装置に入力された複数の入札指標γ_i、識別子ID_iを共有記録媒体に蓄積する過程と、

パラメータｋを下限値ｑにセットする過程と、

全入札装置ｉに$h^{f(n,k)}(IV_i)$の提示を要求する提示要求過程と、

その提示要求を受けた入札装置ｉはその初期値IV_iを用いて$h^{f(n,k)}(IV_i)$（$=D_i$）を生成し、このD_iを開札装置に入力する過程と、

開札装置は入力された全D_iを共有記録媒体に蓄積する過程と、

全D_iに対して、$h^{f(n,q-1)-f(n,k)}(D_i)$を作成する過程と、

これら$h^{f(n,q-1)-f(n,k)}(D_i)$が共有記録媒体上のC_iと各々一致するかを検証する過程と、

その検証で全て一致すると、ｇ（D_i）を生成する過程と、

その各ｇ（D_i）が共有記録媒体上の入札指標γ_iに一致するかを検証する過程と、

その検証でγ_iと一致するものが１つもなければ、共有記録媒体上のC_iをD_iで上書き（$C_i \leftarrow D_i$）し、

ｋを＋１して上記提示要求過程に戻る過程と、

上記検証でγ_iと一致するものがあればその時のｋを落札価格とし、そのｋと、一致したγ_iと対応する入札装置の識別子ID_iとを出力する過程と

を有することを特徴とする請求項５記載の電子競争入札方法。

【請求項１０】　開札装置に入力された複数の入札指標γ_i、識別子ID_iを共有記録媒体に蓄積する過程と、

パラメータｋを上限値ｎにセットする過程と、

全入札装置ｉに価格ｋで入札したかどうか質問する質問過程と、

その質問に対する各入札装置からの応答を開札装置で受信する過程と、

開札装置はこれら応答中に入札したという入札装置があるか検証する過程と、

その検証で入札したという入札装置がなければ、ｋを－１して上記質問過程に戻る過程と、

上記検証で入札したという入札装置があれば、全入札装置に$h^{f(k)}$（IV_i）の提示を要求する過程と、

その提示要求を受けた各入札装置は各々の初期値IV_iを用いて$h^{f(k)}$（IV_i）（＝D_i）を生成し、このD_iを開札装置に入力する過程と、

開札装置は入力された全D_iを共有記録媒体に蓄積する過程と、

上記全D_iに対して、$h^{f(n+1)-f(k)}$（D_i）を作成する過程と、

これら$h^{f(n+1)-f(k)}$（D_i）が共有記録媒体上のC_iと各々一致するかを検証する過程と、

その検証で全て一致すると、入札したという入札装置ｊが提示したD_jに対し、ｇ（D_j）を生成する過程と、

そのｇ（D_j）が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する過程と、

その検証でγ_iと一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する過程と、

を有することを特徴とする請求項２記載の電子競争入札方法。

【請求項１１】　$k \leq t \leq n$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$, $i \neq j$）に対して、　$E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$を作成する過程と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する過程と、

その検証でγ_iと一致するものが１つもなければ、ｋを落札価格とし、そのｋとこの落札価格を提示した入札装置の識別子ID_iとを出力する過程を有することを特徴とした請求項１０記載の電子競争入札方法。

【請求項１２】　開札装置に入力された複数の入札指標γ_i、識別子ID_iを共有記録媒体に蓄積する過程と、

パラメータｋを下限値ｑにセットする過程と、

全入札装置ｉに価格ｋで入札したかどうか質問する質問過程と、

その質問に対する各入札装置からの応答を開札装置で受信する過程と、

開札装置はこれら応答中に入札したという入札装置があるかの検証をする過程と、

その検証で入札したという入札装置がなければ、ｋを＋１して上記質問過程に戻る過程と、

上記検証で入札したという入札装置があれば、全入札装置に$h^{f(n,k)}(IV_i)$の提示を要求する。各入札装置は各々の初期値IV_iを用いて$h^{f(n,k)}(IV_i)$（$=D_i$）を生成し、このD_iを開札装置に入力する過程と、

開札装置は入力された全D_iを共有記録媒体に蓄積する過程と、

上記全D_iに対して$h^{f(n,q-1)-f(n,k)}(D_i)$を作成する過程と、

これら$h^{f(n,q-1)-f(n,k)}(D_i)$が共有記録媒体上のC_iと各々一致するかを検証する過程と、

その検証で全て一致すると、入札したという入札装置ｊが提示したD_jに対し、$g(D_j)$を生成する過程と、

その$g(D_j)$が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかど

うか検証する過程と、

その検証でγ_iと一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する過程と

を有することを特徴とする請求項５記載の電子競争入札方法。

【請求項１３】　$q \leq t \leq k$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$, $i \neq j$）に対して、　$E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$を作成する過程と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する過程と、

その検証でγ_iと一致するものが１つもなければ、ｋを落札価格とし、そのｋと、この落札価格を提示した入札装置の識別子ID_iとを出力する過程を有することを特徴とした請求項１２記載の電子競争入札方法。

【請求項１４】　各入札装置ｉは乱数R_iと入札価格PR_iとを演算したものを一方向性関数ｈ処理して$h(PR_i (+) R_i)$を求める過程を有し、

上記$h(PR_i (+) R_i)$を入札指標γ_iと共に開札装置に入力し、

開札装置に入力されたγ_i，$h(PR_i (+) R_i)$，ID_iを共有記録媒体に蓄積する過程と、

開札装置は全入力が揃うと、全入札装置にPR_iとR_iの提示を要求する過程と、

その提示要求を受けた各入札装置は各々PR_iとR_iを開札装置に入力する過程と、

開札装置はこれら入力されたPR_i，R_iからその最高値ｋと、そのｋを入札した入札装置（落札装置）ｊを決定する過程と、

開札装置は全入札装置に$h^{f(k)}(IV_i)$の提示を要求する過程と、

その提示要求を受けた各入札装置は各々の初期値IV_iを用いて$h^{f(k)}(IV_i)$（$=D_i$）を生成して開札装置に入力する過程と、

開札装置は入力された全D_iを共有記録媒体に蓄積する過程と、

これら全D_iに対して、$h^{f(n+1)-f(k)}(D_i)$を作成する過程と、

これら$h^{f(n+1)-f(k)}(D_i)$が共有記録媒体上のC_iと各々一致するかを検証する過程と、

その検証で全て一致すると、落札装置ｊが提示したD_jに対し、ｇ（D_j）を生成する過程と、

そのｇ（D_j）が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する過程と、

その検証で一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する過程と

を有することを特徴とする請求項２記載の電子競争入札方法。

【請求項１５】　$k \leq t \leq n$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$, $i \neq j$）に対して、$E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$を作成する過程と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する過程と、

その検証で一致するものが１つもなければ、ｋを落札価格とし、そのｋと、この落札価格を提示した入札装置の識別子ID_iを出力する過程を有することを特徴とする請求項１４記載の電子競争入札方法。

【請求項１６】　各入札装置ｉは乱数R_iと入札価格PR_iとを演算したものを一方向性関数ｈ処理してｈ（PR_i（＋）R_i）を求める過程を有し、

上記ｈ（PR_i（＋）R_i）を入札指標γ_iと共に開札装置に入力し、

開札装置に入力されたγ_i、ｈ（PR_i（＋）R_i），ID_iを共有記録媒体に蓄積する過程と、

開札装置は全入力が揃うと、全入札装置にPR_iとR_iの提示を要求する過程と、

その提示要求を受けた各入札装置は各々PR_iとR_iを開札装置に入力する過程と、

開札装置はこれら入力されたPR_i，R_iから、その最低値ｋと、そのｋを入札した入札装置（落札装置）ｊを決定する過程と、

開札装置は全入札装置に$h^{f(n,k)}(IV_i)$の提示を要求する過程と、

その提示要求を受けた各入札装置は各々の初期値IV_iを用いて$h^{f(n,k)}(IV_i)$（＝D_i）を生成し、このD_iを開札装置に入力する過程と、

開札装置は入力された全D_iを共有記録媒体に蓄積する過程と、

上記全D_iに対して、$h^{f(n,q-1)-f(n,k)}$（D_i）を作成する過程と、

これら$h^{f(n,q-1)-f(n,k)}$（D_i）が共有記録媒体上のC_iと各々一致するかを検証する過程と、

その検証で全て一致すると、落札装置ｊが提示したD_jに対し、ｇ（D_j）を生成する過程と、

そのｇ（D_j）が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する過程と、

その検証が一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する過程と

を有することを特徴とする請求項５記載の電子競争入札方法。

【請求項１７】　$q \leq t \leq k$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$, $i \neq j$）に対して、$E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$を作成する過程と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する過程と、

その検証で一致するものが１つもなければ、ｋを落札価格として、そのｋと、この落札価格を提示した入札装置の識別子ID_iを出力する過程を有することを特徴とする請求項１６記載の電子競争入札方法。

【請求項１８】　入札装置はPR_iとR_iの演算に、入札装置ｉが示すこの入札に関する付加情報l_iを加え、ｈ（PR_i（＋）l_i（＋）R_i）を出力し、

開札装置は全入札装置に対しPR_iとR_iのみならずl_iも提示することを要求することを特徴とする請求項１４乃至１７の何れかに記載の電子競争入札方法。

【請求項１９】　入札可能なｎ種類の価格を１，２，…，ｎとし、$1 \leq j \leq n$なるｊに対し、価格ｊを入札しない場合は価格ビット情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、

各入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）は各価格ｊを関数ｆ処理してｆ（ｊ）を求め、各価格ｊごとに価格情報$b_i^{(j)}$を生成し、かつ各価格ｊごとに乱数$R_i^{(j)}$を生成し、

各ｊごとにｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$なる演算を行い、この演算結果を一方向性関数ｈで処理して、その処理結果ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）を上記入札指標とし、

開札装置は各入札装置ｉから入力された｛ID_i，ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）｝を共有記録媒体に蓄積する過程と、

パラメータｋをｎにセットする過程と、

全入札装置に$R_i^{(k)}$の提示を要求する提示要求過程と、

その提示要求された各入札装置は各々$R_i^{(k)}$を開札装置に入力する過程と、

開札装置はその全$R_i^{(k)}$を共有記録媒体に蓄積する過程と、

開札装置は$b_i^{(k)}$＝１として、各ｉに対して入力された$R_i^{(k)}$を用いてｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）を作成する過程と、

これらｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）が共有記録媒体上に一致するものがあるかどうかを検証する過程と、

その検証で一致するものがなければｋを－１して上記提示要求過程に戻る過程と、

上記検証で一致するものがあれば、ｋを落札価格とし、そのｋと、その一致したものの$R_i^{(k)}$を提示した入札装置ｉの識別子ID_iとを出力する過程と

を有することを特徴とする請求項１記載の電子競争入札方法。

【請求項２０】　入札可能なｎ種類の価格を１，２，…，ｎとし、$1 \leq j \leq n$なるｊに対し、価格ｊを入札しない場合は価格情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、

各入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）は各価格ｊを関数ｆ処理してｆ（ｊ）を求め、各価格ｊごとに価格情報$b_i^{(j)}$を生成し、かつ各価格ｊごとに乱数$R_i^{(j)}$を生成し、

各ｊごとにｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$なる演算を行い、この演算結果を一方向性関数ｈで処理して、その処理結果ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（

ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）を上記入札指標とし、

上記乱数$R_i^{(j)}$を開札装置に知らせ、

開札装置は各入札装置から入力された

｛ID_i，ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）｝を共有記録媒体に蓄積する過程と、

パラメータｋをｎにセットする過程と、

全てのｉに対して、$b_i^{(k)}$＝１として、ｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）を作成する指標作成過程と、

そのｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）と一致するものが存在するか検証する過程と、

その検証で一致するものがなければｋを－１して上記指標作成過程に戻る過程と、

上記検証で一致するものがあれば、ｋ′≧ｋである全ての$R_i^{(k')}$を共有記録媒体に蓄積する過程と、

その一致した時のｋを落札価格とし、このｋと一致した時の$R_i^{(k)}$と対応する入札装置の識別子ID_iとを出力する過程と

を有することを特徴とする請求項１記載の電子競争入札方法。

【請求項２１】　入札可能なｎ種類の価格を１，２，…，ｎとし、１≦ｊ≦ｎなるｊに対し、価格ｊを入札しない場合は価格情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、

各入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）は各価格ｊを関数ｆ処理してｆ（ｊ）を求め、各価格ｊごとに価格情報$b_i^{(j)}$を生成し、かつ各価格ｊごとに乱数$R_i^{(j)}$を生成し、

各ｊごとにｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$なる演算を行い、この演算結果を一方向性関数ｈで処理して、その処理結果ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）を上記入札指標とし、

開札装置は各入札装置から入力された

｛ＩＤ$_i$，ｈ（ｆ（１）（＋）ｂ$_i^{(1)}$（＋）Ｒ$_i^{(1)}$），ｈ（ｆ（２）（＋）ｂ$_i^{(2)}$（＋）Ｒ$_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）ｂ$_i^{(n)}$（＋）Ｒ$_i^{(n)}$））｝を共有記録媒体に蓄積する過程と、

パラメータｋを入札可能な最低価格１にセットする過程と、

全入札装置にＲ$_i^{(k)}$の提示を要求する提示要求過程と、

その提示要求された各入札装置は各々Ｒ$_i^{(k)}$を開札装置に入力する過程と、

開札装置はその全Ｒ$_i^{(k)}$を共有記録媒体に蓄積する過程と、

開札装置はｂ$_i^{(k)}$＝１として、各ｉに対して入力されたＲ$_i^{(k)}$を用いてｈ（ｆ（ｋ）（＋）１（＋）Ｒ$_i^{(k)}$）を作成する過程と、

これらｈ（ｆ（ｋ）（＋）１（＋）Ｒ$_i^{(k)}$）が共有記録媒体上に一致するものがあるかどうかを検証する過程と、

その検証で一致するものがなければｋを＋１して上記提示要求過程に戻る過程と、

上記検証で一致するものがあれば、ｋを落札価格とし、そのｋと、その一致したもののＲ$_i^{(k)}$を提示した入札装置の識別子ＩＤ$_i$とを出力する過程と

を有することを特徴とする請求項１記載の電子競争入札方法。

【請求項２２】　入札可能なｎ種類の価格を１，２，…，ｎとし、$1 \leq j \leq n$なるｊに対し、価格ｊを入札しない場合は価格情報ｂ$^{(j)}$を０とし、入札する場合はｂ$^{(j)}$を１とし、

各入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）は各価格ｊを関数ｆ処理してｆ（ｊ）を求め、各価格ｊごとに価格情報ｂ$_i^{(j)}$を生成し、かつ各価格ｊごとに乱数Ｒ$_i^{(j)}$を生成し、

各ｊごとにｆ（ｊ）（＋）ｂ$_i^{(j)}$（＋）Ｒ$_i^{(j)}$なる演算を行い、この演算結果を一方向性関数ｈで処理して、その処理結果ｈ（ｆ（１）（＋）ｂ$_i^{(1)}$（＋）Ｒ$_i^{(1)}$），ｈ（ｆ（２）（＋）ｂ$_i^{(2)}$（＋）Ｒ$_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）ｂ$_i^{(n)}$（＋）Ｒ$_i^{(n)}$）を上記入札指標とし、

上記乱数Ｒ$_i^{(j)}$を開札装置に知らせ、

開札装置は各入札装置から入力された

｛ＩＤ$_i$，ｈ（ｆ（１）（＋）ｂ$_i^{(1)}$（＋）Ｒ$_i^{(1)}$），ｈ（ｆ（２）（＋

）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，h（f（n）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$））｝を共有記録媒体に蓄積する過程と、

パラメータｋを入札可能な最低価格１にセットする過程と、

全てのｉに対して、$b_i^{(k)}$＝１として、h（f（k）（＋）１（＋）$R_i^{(k)}$））を作成する指標作成過程と、

そのh（f（k）（＋）１（＋）$R_j^{(k)}$）と、共有記録媒体上に一致するものが存在するか検証する過程と、

その検証で一致するものがなければｋを＋１して上記指標作成過程に戻る過程と、

上記検証で一致するものがあれば、$k' \leq k$である全ての$R_i^{(k')}$を共有記録媒体に蓄積する過程と、

その一致した時のｋを落札価格とし、このｋと、一致した時の$R_i^{(k)}$と対応する入札装置の識別子ID_iとを出力する過程と、

を有することを特徴とする請求項１記載の電子競争入札方法。

【請求項２３】　入札装置ｉはその識別子ID_iを仮識別子登録装置へ送り、

仮識別子登録装置は識別子ID_iに対し、仮識別子AID_iを発行し、これらの組を記録媒体に保存し、

かつ仮識別子AID_iを入札装置ｉへ送り、

入札装置ｉは開札装置に対し、識別子ID_iとして仮識別子AID_iを入札指標と共に送る

ことを特徴とする請求項１乃至２２の何れかに記載の電子競争入札方法。

【請求項２４】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値をIV_i、入札価格の上限値をｎとする時、各入札装置ｉに対する$C_i = h^{f(n+1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること表わす）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子ID_iと、入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$（g（C）はCを一方向性関数ｇで処理

することを、PR_i は入札装置ｉの入札価格を、ｆ（Ｄ）はＤを変数とする関数を表わす）とを共有記録媒体に蓄積する処理と、

処理パラメータｋを上限値ｎに設定する処理と、

$\delta_i = g(h^{f(k)}(IV_i))$ を各 IV_i について演算する δ_i 演算処理と、

δ_i が共有記録媒体上の入札指標 γ_i と一致するか調べる照合処理と、

上記照合処理で何れの IV_i についても一致するものがなければ上記ｋを－１して上記 δ_i 演算処理に戻る処理と、

上記照合処理で一致すると、その時のｋを落札価格とし、その一致した γ_i と対応する識別子 ID_i とを出力する処理と、

を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項２５】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値を IV_i、入札価格の上限値をｎ、下限値をｑとする時、各入札装置ｉに対する $C_i = h^{f(n,q-1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること、ｆ（Ｃ，Ｄ）はＤが大きくなる程ｆ（Ｃ，Ｄ）の値が小さな正の整数となる関数を表す）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子 ID_i と、入札指標 $\gamma_i = g(h^{f(n,PRi)}(IV_i))$（ｇ（Ｅ）はＥを一方向性関数ｇで処理すること、$PR_i$ は入札装置ｉの入札価格を表わす）とを共有記録媒体に蓄積する処理と、

処理パラメータｋを下限値ｑに設定する処理と、

$\delta_i = g(h^{f(n,k)}(IV_i))$ を各 IV_i について演算する δ_i 演算処理と、

δ_i が共有記録媒体上の入札指標 γ_i と一致するか調べる照合処理と、

上記照合過程で何れの IV_i についても一致するものがなければ上記ｋを＋１して上記 δ_i 演算処理に戻る処理と、

上記照合処理で一致すると、その時のｋを落札価格とし、その一致した γ_i と対応する識別子 ID_i とを出力する処理と

を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項２６】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値をIV_i、入札価格の上限値をｎとする時、各入札装置ｉに対する$C_i = h^{f(n+1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること表わす）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子ID_iと、入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$（ｇ（Ｃ）はＣを一方向性関数ｇで処理すること、$PR_i$は入札装置ｉの入札価格を、ｆ（Ｄ）はＤを変数とする関数を表わす）とを共有記録媒体に蓄積する処理と、

パラメータｋを上限値ｎにセットする処理と、

全入札装置ｉに$h^{f(k)}(IV_i)$の提示を要求する提示要求処理と、

各入札装置ｉから入力される$h^{f(k)}(IV_i)$（$=D_i$）を共有記録媒体に蓄積する処理と、

上記入力された全D_iに対して、$h^{f(n+1)-f(k)}(D_i)$を作成する処理と、

これら$h^{f(n+1)-f(k)}(D_i)$が共有記録媒体上のC_iと各々一致するかを検証する処理と、

その検証で全て一致すると、ｇ（D_i）を生成する処理と、

その各ｇ（D_i）が共有記録媒体上の入札指標γ_iに一致するかを検証する処理と、

その検証で一致するものが１つもなければ、共有記録媒体上のC_iをD_iで上書き（$C_i \leftarrow D_i$）し、ｋを－１して上記提示要求処理に戻る処理と、

上記検証で一致するものがあればその時のｋを落札価格とし、そのｋと、この落札価格を提示した入札装置の識別子ID_iとを出力する処理と、

上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項２７】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値をIV_i、入札価格の上限値をｎ、下限値をｑとする時、各入札装置ｉに対する$C_i = h^{f(n,q-1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること、ｆ（Ｃ，Ｄ）はＤが大きくなる程ｆ（Ｃ，Ｄ）の値が小さな正の整数となる関数を表す）を共有記録媒体に蓄積した開札装置のコンピュータが

実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子$ＩＤ_i$と、入札指標$\gamma_i = g(h^{f(n,PRi)}(ＩＶ_i))$（ｇ（Ｅ）はＥを一方向性関数ｇで処理すること、$ＰＲ_i$は入札装置ｉの入札価格を表わす）とを共有記録媒体に蓄積する処理と、

パラメータｋを下限値ｑにセットする処理と、

全入札装置ｉに$h^{f(n,k)}(ＩＶ_i)$の提示を要求する提示要求処理と、

各入札装置ｉより入力された$h^{f(n,k)}(ＩＶ_i)$（$＝Ｄ_i$）を共有記録媒体に蓄積する処理と、

上記入力された全$Ｄ_i$に対して、$h^{f(n,q-1)-f(n,k)}(Ｄ_i)$を作成する処理と、

これら$h^{f(n,q-1)-f(n,k)}(Ｄ_i)$が共有記録媒体上の$Ｃ_i$と各々一致するかを検証する処理と、

上記検証で全て一致すると、ｇ（$Ｄ_i$）を生成する処理と、

これら各ｇ（$Ｄ_i$）が共有記録媒体上の入札指標γ_iに一致するかを検証する処理と、

その検証で一致するものが１つもなければ、共有記録媒体上の$Ｃ_i$を$Ｄ_i$で上書き（$Ｃ_i \leftarrow Ｄ_i$）し、ｋを＋１として上記提示要求処理に戻る処理と、

上記検証で一致するものがあれば、その時のｋを落札価格とし、そのｋと、一致したγ_iと対応した入札装置の識別子$ＩＤ_i$とを出力する処理と、

上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項２８】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値を$ＩＶ_i$、入札価格の上限値をｎとする時、各入札装置ｉに対する$Ｃ_i = h^{f(n+1)}(ＩＶ_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること表わす）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子$ＩＤ_i$と、入札指標$\gamma_i = g(h^{f(PRi)}(ＩＶ_i))$（ｇ（Ｃ）はＣを一方向性関数ｇで処理すること、$ＰＲ_i$は入札装置ｉの入札価格を、ｆ（Ｄ）はＤを変数とする関数を

表わす）とを共有記録媒体に蓄積する処理と、

パラメータｋを上限値ｎにセットする処理と、

全入札装置ｉに価格ｋで入札したかどうか質問する質問処理と、

その質問に対する入札装置からの応答を入力する処理と、

その入力された応答中に入札したという入札装置があるか検証する処理と、その検証で入札したという入札装置がなければ、ｋを－１して上記質問処理に戻る処理と、

上記検証で入札したという入札装置があれば、全入力装置に$h^{f(k)}$（IV_i）の提示を要求する処理と、

各入札装置から入力された$h^{f(k)}$（IV_i）（＝D_i）を共有記録媒体に蓄積する処理と、

上記入力された全D_iに対して、$h^{f(n+1)-f(k)}$（D_i）を作成する処理と、

これら$h^{f(n+1)-f(k)}$（D_i）が共有記録媒体上のC_iと各々一致するかを検証する処理と、

その検証で全て一致すると、入札したという入札装置ｊが提示したD_jに対し、ｇ（D_j）を生成する処理と、

そのｇ（D_j）が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する処理と、

$k \leq t \leq n$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$，$i \neq j$）に対して、$E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$を作成する処理と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する処理と、

その検証で一致するものが１つもなければ、その時のｋを落札価格とし、そのｋと、上記一致したγ_iと対応した入札装置の識別子ID_iとを出力する処理とを上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項２９】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値をIV_i、入札価格の上限値をｎ、下限値をｑとする時、各入札装置ｉに対する$C_i = h^{f(n,q-1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈ

で処理すること、ｆ（Ｃ，Ｄ）はＤが大きくなる程ｆ（Ｃ，Ｄ）の値が小さな正の整数となる関数を表す）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子$ＩＤ_i$と、入札指標$\gamma_i = g(h^{f(n,PRi)}(ＩＶ_i))$（ｇ（Ｅ）はＥを一方向性関数ｇで処理すること、$ＰＲ_i$は入札装置ｉの入札価格を表わす）とｈ（$ＰＲ_i$（＋）$Ｒ_i$）（$Ｒ_i$は乱数、（＋）は演算を表わす）とを共有記録媒体に蓄積する処理と、

パラメータｋを下限値ｑにセットする処理と、

全入札装置ｉに価格ｋで入札したかどうか質問する質問処理と、

その質問に対する各入札装置からの応答を入力する処理と、

これら応答中に入札したという入札装置があるかの検証をする処理と、

その検証で入札したという入札装置がなければ、ｋを＋１して上記質問処理に戻る処理と、

上記検証で入札したという入札装置があれば、全入力装置に$h^{f(n,k)}(ＩＶ_i)$の提示を要求する処理と、

各入札装置からの$h^{f(n,k)}(ＩＶ_i)$（＝$Ｄ_i$）を入力する処理と、

その入力された全$Ｄ_i$を共有記録媒体に蓄積する処理と、

上記入力された全$Ｄ_i$に対して$h^{f(n,q-1)-f(n,k)}(Ｄ_i)$を作成する処理と

これら$h^{f(n,q-1)-f(n,k)}(Ｄ_i)$が共有記録媒体上の$Ｃ_i$と各々一致するかを検証する処理と、

その検証で全て一致すると、入札したという入札装置ｊが提示した$Ｄ_j$に対し、$g(Ｄ_j)$を生成する処理と、

その$g(Ｄ_j)$が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する処理と、

$q \leq t \leq k$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$，$i \neq j$）に対して、$E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(ＩＶ_i)))$を作成する処理と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する過程と、

その検証で一致するものが１つもなければ、その時のｋを落札価格とし、そのｋと、上記一致したγ_iと対応した入札装置の識別子ID_iとを出力する処理とを上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項３０】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値をIV_i、入札価格の上限値をｎとする時、各入札装置ｉに対する$C_i = h^{f(n+1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること表わす）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子ID_iと、入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$（ｇ（Ｃ）はＣを一方向性関数ｇで処理すること、$PR_i$は入札装置ｉの入札価格を、ｆ（Ｄ）はＤを変数とする関数を表わす）とｈ（PR_i（＋）R_i）（R_iは乱数、（＋）は演算を表わす）とを共有記録媒体に蓄積する処理と、

全入力が揃うと、全入札装置にPR_iとR_iの提示を要求する処理と、

各入札装置ｉからのPR_iとR_iを入力する処理と、

これら入力されたPR_i，R_iからその最高値ｋと、ｋを入札した入札装置（落札装置）ｊを決定する処理と、

全入札装置に$h^{f(k)}(IV_i)$の提示を要求する処理と、

各入札装置ｉからの$h^{f(k)}(IV_i)$（＝D_i）を入力して共有記録媒体に蓄積する処理と、

上記入力した全D_iに対して、$h^{f(n+1)-f(k)}(D_i)$を作成する処理と、

これら$h^{f(n+1)-f(k)}(D_i)$が共有記録媒体上のC_iと各々一致するかを検証する処理と、

その検証で全て一致すると落札装置ｊが提示したD_jに対し、ｇ（D_i）を生成する処理と、

ｇ（D_j）が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する処理

と、

ｋ≦ｔ≦ｎであるｔと、ｊを除く全てのｉ（１≦ｉ≦ｍ，ｉ≠ｊ）に対して、$E_i = g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$を作成する処理と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する処理と、

その検証で一致するものが１つもなければ、そのｋを落札価格とし、そのｋとの落札価格を提示した入札装置の識別子ID_iとを出力する処理と

をコンピュータに実行させるプログラムを記録した記録媒体。

【請求項３１】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）に固有の初期値をIV_i、入札価格の上限値をｎ、下限値をｑとする時、各入札装置ｉに対する$C_i = h^{f(n,q-1)}(IV_i)$（h^A（Ｂ）はＢをＡ回一方向性関数ｈで処理すること、ｆ（Ｃ，Ｄ）はＤが大きくなる程ｆ（Ｃ，Ｄ）の値が小さな正の整数となる関数を表す）を共有記録媒体に蓄積した開札装置のコンピュータが実行するプログラムを記録した記録媒体であって、

各入札装置ｉから入力された、その入札装置ｉを特定する識別子ID_iと、入札指標$\gamma_i = g(h^{f(n,PRi)}(IV_i))$（ｇ（Ｅ）はＥを一方向性関数ｇで処理すること、$PR_i$は入札装置ｉの入札価格を表わす）とｈ（$PR_i$（＋）$R_i$）（$R_i$は乱数、（＋）は演算を表わす）とを共有記録媒体に蓄積する処理と、

全入力が揃うと、全入札装置にPR_iとR_iの提示を要求する処理と、

各入札装置ｉからのPR_iとR_iを入力する処理と、

これら入力されたPR_i，R_iからその最低値ｋと、ｋを入札した入札装置（落札装置）ｊを決定する処理と、

全入札装置に$h^{f(n,k)}(IV_i)$の提示を要求する処理と、

各入札装置ｉからの$h^{f(n,k)}(IV_i)$（＝D_i）を入力してその全D_iを共有記録媒体に蓄積する処理と、

上記入力された全D_iに対して、$h^{f(n,q-1)-f(n,k)}(D_i)$を作成する処理と、

これら$h^{f(n,q-1)-f(n,k)}(D_i)$が共有記録媒体上のC_iと各々一致するかを検証する処理と、

その検証で全て一致すると落札装置ｊが提示したD_jに対し、ｇ（D_j）を生

成する処理と、

そのｇ（D_i）が共有記録媒体上の入札装置ｊの入札指標γ_jに一致するかどうか検証する処理と、

その検証で一致すれば、確かに入札装置ｊは価格ｋで入札したと判断する処理と、

ｑ≦ｔ≦ｋであるｔと、ｊを除く全てのｉ（１≦ｉ≦ｍ，ｉ≠ｊ）に対して、$E_i = g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(ID_i)))$を作成する処理と、

これらE_iが共有記録媒体上の入札指標γ_iと一致するかを検証する処理と、

その検証で一致するものが１つもなければ、そのｋを落札価格ｋとし、このｋとこの落札価格を提示した入札装置の識別子ID_iとを出力する処理と

を上記コンピュータに実行させるプログラムを記録した記録媒体。

【請求項３２】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）を特定する識別子をID_iとし、入札可能なｎ種類の価格を１，２，…，ｎとし、１≦ｊ≦ｎなる価格ｊを入札しない場合は価格ビット情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、一方向性関数ｈでＡを処理することをｈ（Ａ）とし、ＢとＣの演算をＢ（＋）Ｃとし、

Ｄを変数とする関数をｆ（Ｄ）とし、$R_i^{(j)}$を乱数とし、上記乱数$R_i^{(j)}$は開札装置に知らせてあり、

各入札装置ｉから入力された

$\{ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}), h(f(2)(+)b_i^{(2)}(+)R_i^{(2)}), \cdots, h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})\}$を共有記録媒体に蓄積する処理と、

パラメータｋをｎに設定する処理と、

全入札装置に$R_i^{(k)}$の提示を要求する提示要求処理と、

各入札装置ｉからの$R_i^{(k)}$を入力して共有記録媒体に蓄積する処理と、

$b_i^{(k)}$＝１として、各ｉに対して上記入力された$R_i^{(k)}$を用いてｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）を作成する処理と、

これらｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）と一致するものが共有記録媒体上にあるかどうかを検証する処理と、

その検証で一致するものがなければｋを－１して上記提示要求処理に戻る処理と、

上記検証で一致するものがあれば、その時のｋを落札価格とし、そのｋと、一致した時の$R_i^{(k)}$と対応した入札装置の識別子ID_iを出力する処理と

を開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項３３】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）を特定する識別子をID_iとし、入札可能なｎ種類の価格を１，２，…，ｎとし、$1 \leq j \leq n$なる価格ｊを入札しない場合は価格ビット情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、一方向性関数ｈでＡを処理することをｈ（Ａ）とし、ＢとＣの演算をＢ（＋）Ｃとし、

Ｄを変数とする関数をｆ（Ｄ）とし、$R_i^{(j)}$を乱数とし、上記乱数$R_i^{(j)}$は開札装置に知らせてあり、

各入札装置ｉから入力された｛ID_i，ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）｝を共有記録媒体に蓄積する処理と、

パラメータｋをｎにセットする処理と、

全てのｉに対して、$b_i^{(k)}$＝１として、ｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）を作成する指標作成処理と、

そのｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）と一致するものが共有記録媒体上に存在するか検証する処理と、

その検証で一致するものがなければｋを－１して上記指標作成処理に戻る処理と、

上記検証で一致するものがあれば、$k' \geq k$である全ての$R_i^{(k')}$を共有記録媒体に蓄積する処理と、

その一致した時のｋを落札価格とし、そのｋと、一致した時の$R_i^{(k)}$と対応する入札装置の識別子ID_iとを出力する処理と、

を上記開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項３４】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）を特定する識別子をID_iとし、入札可能なｎ種類の価格を１，２，…，ｎとし、１

≦ｊ≦ｎなる価格ｊを入札しない場合は価格ビット情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、一方向性関数ｈでＡを処理することをｈ（Ａ）とし、ＢとＣの演算をＢ（＋）Ｃとし、

Ｄを変数とする関数をｆ（Ｄ）とし、$R_i^{(j)}$を乱数とし、

各入札装置ｉから入力された｛ID_i，ｈ（ｆ（ｉ）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）｝を共有記録媒体に蓄積する処理と、

パラメータｋを入札可能な最低価格１にセットする処理と、

全入札装置に$R_i^{(k)}$の提示を要求する提示要求処理と、

各入札装置ｉからの$R_i^{(k)}$を入力して共有記録媒体に蓄積する処理と、

$b_i^{(k)}$＝１として、各ｉに対して入力された$R_i^{(k)}$を用いてｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）を作成する処理と、

これらｈ（ｆ（ｋ）（＋）１（＋）$R_i^{(k)}$）と一致するものが共有記録媒体上にあるかどうかを検証する処理と、

その検証で一致するものがなければｋを＋１として上記提示要求処理に戻る処理と、

上記検証で一致するものがあれば、その時のｋを落札価格とし、そのｋと、一致したものの$R_i^{(k)}$と対応した入札装置の識別子ID_iとを出力する処理とを開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項３５】　入札装置ｉ（ｉ＝１，２，…，ｍ、ｍは入札参加数）を特定する識別子をID_iとし、入札可能なｎ種類の価格を１，２，…，ｎとし、１≦ｊ≦ｎなる価格ｊを入札しない場合は価格ビット情報$b^{(j)}$を０とし、入札する場合は$b^{(j)}$を１とし、一方向性関数ｈでＡを処理することをｈ（Ａ）とし、ＢとＣの演算をＢ（＋）Ｃとし、

Ｄを変数とする関数をｆ（Ｄ）とし、$R_i^{(j)}$を乱数とし、上記乱数$R_i^{(j)}$は開札装置に知らせてあり、

各入札装置ｉから入力された｛ID_i，ｈ（ｆ（１）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），ｈ（ｆ（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，ｈ（ｆ（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）｝を共有記録媒体に蓄積する処理と、

パラメータｋを入札可能な最低価格１にセットする処理と、

全てのｉに対して、$b_i^{(k)}$＝１として$h(f(k)(+)1(+)R_i^{(k)})$を作成する指標作成処理と、

その$R(f(k)(+)1(+)R_i^{(k)})$と一致するものが共有記録媒体上に存在するか検証する処理と、

その検証で一致するものがなければｋを＋１して上記指標作成処理に戻る処理と、

上記検証で一致するものがあれば、$k' \leq k$である全ての$R_i^{(k')}$を共有記録媒体に蓄積する処理と、

その一致した時のｋを落札価格とし、そのｋと、一致した時の$R_i^{(k)}$と対応する入札装置の識別子ID_iとを出力する処理と

を上記開札装置のコンピュータに実行させるプログラムを記録した記録媒体。

【請求項３６】　電子競争入札システムの入札装置であって、

入札価格を生成する入札価格生成装置と、

上記生成された入札価格を一方向性関数を用いて入札指標に変換する入札価格変換装置と、

上記入札指標と、入札装置を特定する識別子とを開札装置へ送る手段と

を具備することを特徴とする入札装置。

【請求項３７】　上記入札価格変換装置は、上記入札価格PR_iを変数として$f(PR_i)$を出力する関数ｆ処理装置と、

上記入札装置に固有の初期値IV_iを、上記$f(PR_i)$回だけ一方向性関数ｈで処理して$h^{f(PRi)}(IV_i)$を出力する一方向性関数ｈ処理装置と、

上記一方向性関数ｈ処理装置の出力を一方向性関数ｇで処理して上記入札指標を得る一方向性関数ｇ処理装置と

よりなることを特徴とする請求項３６記載の入札装置。

【請求項３８】　上記入札価格変換装置は、上記入札価格PR_iと入札価格の上限値ｎとを変数として、入力し、PR_iが大きい程、小さい正の整数値$f(n, PR_i)$を出力する関数ｆ処理装置と、

上記入札装置に固有の初期値IV_iを、上記$f(n, PR_i)$回だけ一方向性

関数ｈで処理して$h^{f(n,PRi)}$（IV_i）を出力する一方向性関数ｈ処理装置と、

上記一方向性関数ｈ処理装置の出力を一方向性関数ｇで処理して上記入札指標を得る一方向性関数ｇ処理装置と

よりなることを特徴とする請求項３６記載の入札装置。

【請求項３９】　乱数R_iを生成する乱数生成装置と、

上記乱数R_iと上記入札価格PR_iとを演算してPR_i（＋）R_iを出力する演算装置と、

上記PR_i（＋）R_iを一方向性関数ｈで処理してｈ（PR_i（＋）R_i）を出力する一方向性関数ｈ処理手段と、

を備え、上記ｈ（PR_i（＋）R_i）をも上記入札指標と共に出力することを特徴とする請求項３７又は３８記載の入札装置。

【請求項４０】　上記入札価格変換装置は、

入札可能なｎ種類の価格１，２，…，ｎの$1 \leq j \leq n$なるｊに対し、価格ｊを入札しない場合は価格ビット情報$b^{(j)}$を０とし、価格ｊを入札する場合は$b^{(j)}$を１として出力する$b_j^{(j)}$生成装置と、

入札装置ｉ及び価格ｊに固有な乱数$R_i^{(j)}$を生成する乱数生成装置と、

価格ｊを変数とする関数ｆ（ｊ）を出力する関数ｆ処理装置と、

上記ｆ（ｊ）と上記$R_i^{(j)}$と上記$b_i^{(j)}$を入力して演算ｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$を行う演算装置と、

上記ｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$を一方向性関数ｈで処理してｈ（ｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$）を出力する一方向性関数ｈ処理装置と、

上記価格ｊの１～ｎのそれぞれについて上記ｈ（ｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$）を求めて、これらｎ個を上記入札指標とする制御装置と

よりなることを特徴とする請求項３６記載の入札装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は情報セキュリティ技術を応用して、特にインターネットなどにより

多数の入札者がオンラインでアクセス可能な状況下で、競争入札を実現する方法、その装置及びプログラム記録媒体に関するものである。

【０００２】

【従来の技術】

従来の電子競争入札の方法の構成を図１に挙げる。従来の方法では入札公告が各入札装置11_1～11_mに与えられ、各入札装置11_1～11_mはそれぞれその装置の識別子と入札価格とを開札装置１２へ送信する。この各データ転送の際に、データを暗号化やデジタル署名が添付され送られていた。開札装置１２は各入札装置から受信した入札価格中の最大値（又は最小値）を探し、その値と対応する識別子を出力する。この技術の例として太田と岡本による「電子式入札システム」特開平２－１１８８７６号がある。一方、落札価格のみが公となり、これ以外は秘匿可能な技術として以下が挙げられる。

・佐古、「落札値以外を秘匿する全体検証可能な電子入札方式」、暗号と情報セキュリティシンポジウムＳＣＩＳ’９９.

・宮崎、櫻井、「公開掲示版を用いた秘策可能な電子入札システム」、暗号と情報セキュリティシンポジウムＳＣＩＳ’９９.

などに示されている。

【０００３】

この発明が対象としている入札方法は次のことを条件としている。

・いかなる入札装置も参加可能である。

・入札価格を落札の唯一の判断材料とし、これ以外の情報では落札した入札装置は決定されない。

・開札装置および仮識別子登録装置は不正を働かず、かつ誤動作を起こさない。

・落札した入札装置からの落札価格支払と落札商品の受渡しに関してはこの装置は関与しない。

【０００４】

【発明が解決しようとする課題】

入札前に他の入札装置の情報を得、有利に入札を行うことを防止（公平性）。

落札価格と決定に関する不正防止（正当性）。

開札時にその価格で入札したことを認めない行為防止（否認不可性）。

各入札装置の識別子情報漏洩防止（匿名性）。

【０００５】

同一入札装置による複数回の入札防止。

【０００６】

【課題を解決するための手段】

この発明によれば入札装置において、入札価格と、一方向性関数を利用して入札指標に変換し、開札装置では、その入札指標を利用して、非落札価格を全入札装置に知らせることなく落札価格を決める。

【０００７】

【発明の実施の形態】

実施例１

電子競争入札装置は図１に示した場合と同様にｍ個の入札装置11_1～11_mと開札装置１２とから成り、これら間に相互に通信可能とする。

この装置は、図２に示す流れに従って動作する。

【０００８】

Ｓｔｅｐ１：各入札装置11_1～11_mに入札公告を入力する。

Ｓｔｅｐ２：各入札装置11_i（ｉ＝１，２，…，ｍ）は入力である入札の内容を記述された入札公告に対して、入札価格を生成し、入札価格と自分を特定できる識別子を開札装置１２に送信する。

Ｓｔｅｐ３：開札装置１２は入力である複数の入札価格と各々に対応した識別子に対して、全入札価格中の最大値（または最小値）を求めて落札価格を決める。

【０００９】

Ｓｔｅｐ４：その落札価格とこれを提示した入札装置の識別子を出力する。

入札指標

以上の処理は従来技術と同様である。このような処理では各入札装置は他の入札装置の入札価格を知ることができる。そこでこの発明では入札価格を入札指標に変換して用いる。

【００１０】

図３に示すように、入札装置11_i内において入札価格生成装置１３より生成された入札価格は入札価格変換装置１４に入力され、一方向性関数を用いて整数の入札指標に変換して出力し、この入札指標と識別子を開札装置１２へ送る。開札装置１２は全入札指標から落札価格を決める。

入札価格変換装置１４は図４に示すように入札価格生成装置１３から初期値IV_iと、入札価格PR_iが入力され、IV_iを初期値として、これに対し、PR_iに応じた関数だけ一方向性関数演算がなされる。一方向性関数はｘが与えられたとき、ｘからｙ（＝ｈ（ｘ））を求めることは容易であるが、逆にｙが与えられた時に、ｙ＝ｈ（ｘ）となるｘを求めるのは計算量が極めて大きなものである。またｈ（…ｈ（ｈ（ｈ（IV_i））…）のように初期値IV_iを関数ｈでｋ回処理した出力値をh^k（IV_i）と表わす。

【００１１】

入札価格変換装置１４の具体例を図５に、その処理手順を示す。

Ｓｔｅｐ１：入札価格PR_iと初期値IV_iを入力する。

Ｓｔｅｐ２：関数ｆ処理装置１５でPR_iに対し、関数演算ｆ（PR_i）を行う。ｆ（PR_i）は例えば入札価格が１００円、２００円、３００円…の場合にPR_i／１００の演算を行い、ｆ（PR_i）は１，２，３，…となり処理が簡単になる。

【００１２】

Ｓｔｅｐ３：一方向性関数ｈ処理装置１６において、変数ｔを０とし、初期値IV_iをγ_iとし、以下のＳｔｅｐ４とＳｔｅｐ５を繰返す。

Ｓｔｅｐ４：ｔがｆ（PR_i）以下であるかを判定し、

Ｓｔｅｐ５：ｔ$\leq$ｆ（PR_i）であればその時のｈ（γ_i）をγ_iとし、またｔを＋１してステップＳ４に戻る。

【００１３】

Ｓｔｅｐ６：ｔ$\leq$ｆ（PR_i）でなくなると、その時は$\gamma_i = h^{f(PRi)}$（IV_i）であり、これを一方向性関数ｇ処理装置１７で処理しγ_i＝ｇ（γ_i）とする。

Ｓｔｅｐ７：そのγ_iを入札指標として出力する。

開札装置（最高値落札）

図７に開札装置１２の構成を示す。その装置１２は制御装置２１と、この制御装置２１にそれぞれ接続された一方向性関数ｈ処理装置２２、一方向性関数ｇ処理装置２３、減算器２４、記録媒体２５、関数ｆ処理装置２６と、メモリ手段３５とから成る、関数ｆ処理装置２６、一方向性関数ｈ処理装置２２、一方向性関数ｇ処理装置２３は順次直列に接続されている。また記録媒体２５以外の部分は落札価格選択装置２７を構成する。各入札装置11_iの初期値IV_iは予め何らかの手段により開札装置１２の記録媒体２５に記録されている。

【００１４】

この装置の動作の手順を図８に示す。この例は最高の入札価格を落札価格とする場合である。

Ｓｔｅｐ１：制御装置２１は外部から入力された入札指標γ_i，識別子ID_iを他の装置から参照可能な共有の記録媒体２５に記録する。

Ｓｔｅｐ２：制御装置２１は記録媒体２５から入札価格の上限値ｎをメモリ手段３５から読み出し、ｋにｎを代入する。

【００１５】

Ｓｔｅｐ３：制御装置２１はｋ＞０かを判定し、

Ｓｔｅｐ４：ｋ＞０であれば、ｉを１とし、

Ｓｔｅｐ５：ｉ＞ｍかを判定し、

Ｓｔｅｐ６：ｉ＞ｍでなければｔを０とし、IV_iを記録媒体２５から読出して$\delta_i = IV_i$とする。

【００１６】

Ｓｔｅｐ７：制御装置２１は関数ｆ処理装置２６にｋを入力してｆ（ｋ）を求める。

Ｓｔｅｐ８：制御装置２１は一方向性関数ｈ処理装置２２にδ_iとｆ（ｋ）を入力して、δ_iを初期値として、これをｆ（ｋ）回、一方向性関数ｈで処理して$\delta_i = h^{f(k)}(IV_i)$を求める。

【００１７】

Ｓｔｅｐ９：一方向性関数ｈ処理装置２２の出力$\delta_i = h^{f(k)}(IV_i)$を一方向性関数ｇ処理装置２３に入力して、一方向性関数ｇで処理して$\delta_i = g(h^{f(k)}(IV_i))$を出力する。

Ｓｔｅｐ１０：制御装置２１は$\delta_i = g(h^{f(k)}(IV_i))$と同じ値が記録媒体２５上の$\gamma_i$中に存在するかの照合を行う。

【００１８】

Ｓｔｅｐ１１：記録媒体２５上にδ_iと同一のγ_iが存在しなければｉを＋１してスナップＳ５に戻り次のIV_iについて同様のことを行う。

Ｓｔｅｐ１２：ステップＳ５でｉがｍより大になると制御装置２１はｋを減算器２４に入力して、ｋから１を減算して（ｋ←ｋ－１）として、ステップＳ３に進み、減算されたｋについて、$\delta_i = g(h^{f(k)}(IV_i))$と同一の$\gamma_i$が記録媒体２５にあるかの検査を同様に行う。

【００１９】

Ｓｔｅｐ１３：ステップＳ１０でδ_iと同じ値のγ_iが記録媒体２５上に存在すれば、制御装置２１はこれを落札価格と見なし、この時のｋと、合致したγ_iに対応するID_iとを出力して終了する。

なおステップＳ３でｋ＞０でなくなれば、その時の入札価格IV_iは全て上限値ｎ以上であったことになり、その競争入札は落札がなかったことになる。

【００２０】

以上のようにして、上限値ｎの入札価格IR_iがあるかをまず調べ、なければｎから単位値１を減算した値の入札価格IR_iがあるか調べ、なければ、更に単位値１を減算した値について調べると、順次低い値で入札価格IR_iがあるかを調べて行くことにより、最高の入札価格IR_iを探すことができる。

また、各入札装置11_iが$h^{f(n+1)}(IV_i)$を予め公開しておき、開札装置１２が落札価格ｋ、ID_iの他に$h^{f(k)}(IV_i)$も公開すると、その$h^{f(k)}(IV_i)$に対し、ｆ（ｎ＋１）－ｆ（ｋ）回一方向性関数ｈの処理を行ってその値$h^{f(n+1)-f(k)}\ h^{f(k)}(IV_i)$が公開されている$h^{f(n+1)}(IV_i)$と一致すれば、その開札処理が正しく行われたことを納得することができる。

【００２１】

次に最低の入札価格を落札価格とする場合に用いる入札指標を生成する入札価格変換装置１４の例を図９に示す。この場合も関数ｆ処理装置３１と、一方向性関数ｈ処理装置１６と、一方向性関数ｇ処理装置とを備え、更にメモリ手段３２を備えている。メモリ手段３２には入札価格の上限値ｎが格納され、関数ｆ処理装置３１には入札価格PR_iの他に上限値ｎも入力される。関数ｆ処理装置３１はPR_iとｎを変数とする関数ｆ（ｎ，PR_i）を生成する。関数ｆ（ｎ，PR_i）は、（ｎ－PR_i）やｎ／PR_iなどのようにPR_iが大きい程、小さな正の整数値となるような関数である。

【００２２】

この装置は図６に示した動作と同様な動作を行う。ただステップＳ２で入札価格PR_iと、メモリ手段３２から読み出したｎとからｆ（ｎ，α_i）を生成し、以下、図６中のｆ（PR_i）の代りにｆ（ｎ，PR_i）が用いられる。従って一方向性関数ｈ処理装置１６は$h^{f(n,PRi)}$（IV_i）を出力し、一方向性関数ｇ処理装置１７はｇ（$h^{f(n,PRi)}$（IV_i））を出力する。

【００２３】

開札装置（最低値落札）

次に図９に示した入札価格変換装置により生成された入札指標を入力とし、最低入札価格を落札価格とする開札装置１２を図１０に示す。図９において図７と対応する部分に同一番号を付けてある。関数ｆ処理装置２６の代りに、ｎとｋを入力し、ｆ（ｎ，ｋ）を生成する関数ｆ処理装置３３が用いられ、また減算器２４の代りにｋを＋１する加算器３４が用いられている点が異なる。

【００２４】

この装置は図１１に示すように実行される。入札指標γ_i＝ｇ（$h^{f(n,IRi)}$（IV_i））におけるｆ（ｎ，IR_i）はこの例ではｎ－IR_iとする。

Ｓｔｅｐ１：制御装置２１は外部から入力された各入札指標γ_i，と対応識別子ID_iを記録媒体２５に記録する。

Ｓｔｅｐ２：制御装置２１は記録媒体２５から落札上限値ｎと落札下限値ｑをメモリ手段３５から読み出し、ｋにｑを代入する。

Ｓｔｅｐ３：制御装置２１はｎ＞ｋかを判定し、

Ｓｔｅｐ４：ｎ＞ｋであればｉを１とし、

Ｓｔｅｐ５：ｉ＞ｍかを判定し、

Ｓｔｅｐ６：ｉ＞ｍでなければｔを０とし、$ＩＶ_i$ を記録媒体２５から読出して $\delta_i = ＩＶ_i$ とする。

Ｓｔｅｐ７：制御装置２１は関数ｆ処理装置３３にｎ，ｋを入力してｆ（ｎ，ｋ）を求める。この例ではｆ（ｎ，ｋ）＝ｎ－ｋである。

Ｓｔｅｐ８：制御装置２１は一方向性関数ｈ処理装置２２に δ_i とｆ（ｎ，ｋ）を入力して、δ_i を初期値として、これをｆ（ｎ，ｋ）回、一方向性関数ｈで処理して $\delta_i = h^{f(n,k)}(ＩＶ_i)$ を求める。

Ｓｔｅｐ９：一方向性関数ｈ処理装置２２の出力 $\delta_i = h^{f(n,k)}(ＩＶ_i)$ を、一方向性関数ｇ処理装置２３に入力して、一方向性関数ｇで処理して $\delta_i = g(h^{f(n,k)}(ＩＶ_i))$ を出力する。

Ｓｔｅｐ１０：制御装置２１は $\delta_i = g(h^{f(n,k)}(ＩＶ_i))$ と同じ値が記録媒体２５上の γ_i 中に存在するかの照合を行う。

Ｓｔｅｐ１１：記録媒体２５上に δ_i と同一の γ_i が存在しなければｉを＋１してステップＳ５に戻り、次の $ＩＶ_i$ について同様のことを行う。

Ｓｔｅｐ１２：ステップＳ５でｉ＞ｍとなると制御装置２１はｋを加算器３４に入力してｋを＋１して（ｋ←ｋ＋１）として、ステップＳ３に戻り、加算されたｋについて $\delta_i = g(h^{f(n,k)}(ＩＶ_i))$ と同一の γ_i が記録媒体２５上にあるかの検査を同様に行う。

Ｓｔｅｐ１３：ステップＳ１０で δ_i と同じ値の γ_i が記録媒体上に存在すれば、制御装置２１はこれを落札価格と見なし、この時のｋと、合致した γ_i に対応する $ＩＤ_i$ とを出力して終了する。

【００２５】

なおステップＳ３でｎ＞ｋでなくなれば、その時の入札価格 $ＩＶ_i$ は全て下限値ｑ以下か、上限値ｎ以上であったことになり、その競争入札は落札がなかったことになる。

以上のようにしてまずｋを下限値ｑとし、ｑと同一の入札価格 $ＰＲ_i$ があるかを調べ、なければｋを単位値１だけ大として入札価格 $ＰＲ_i$ があるかを調べるこ

とを順次行うことにより、最低の入札価格、つまり落札価格をもとめることができる。

【００２６】

このように$h^{f(n,k)}$（IV_i）とし、ｋ＝ｑ（下限値）から調べるが、一方向性関数ｈの処理回数ｆ（ｎ，ｋ）は大きな値から、対応する入札指標γ_iがあるかを調べているため、他の入札装置の入札価格が知られることがない。つまり$h^{f(k)}$（IV_i）とし、ｋ＝ｑから調べて、最低価格と対応するγ_iを探す場合は、一方向性関数は処理回数が少い値から回数が多い値は容易に求めることができるため、他の入札装置の入札価格を求めることができるおそれがある。

実施例２

上述では開札装置１２は各入札装置11_iの初期値IV_iを知っている必要があった。実施例２では開札装置１２は初期値IV_iを知る必要がない。

【００２７】

最高価格を落札価格とする場合についてまず述べる。

開札装置１２は図１２に示すように、制御装置２１、一方向性関数ｈ処理装置２２、一方向性関数ｇ処理装置２３、減算器２４、メモリ手段３５、および他の装置からも参照可能な共有記録媒体２５から構成されている。

この開札装置１２は図１３に示すように動作する。

【００２８】

まず開札装置に入力された複数の入札データ（入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$、識別子$ID_i$）が共有記録媒体２５に蓄積される（Ｓ１）。また全入札装置と共有されている$h^{f(n+1)}$（IV_i）は予めC_iとして共有記録媒体２５に蓄積されている。ここではｍ個の入札があったとし、ｉ＝１，２，…，ｍとする。カウンタの計数値ｋを上限値ｎにセットする（Ｓ２）。

【００２９】

全入札装置11_iに$h^{f(k)}$（IV_i）の提示を要求する（Ｓ３）。各入札装置11_iは各々の初期値IV_iを用いて$h^{f(k)}$（IV_i）（$=D_i$）を生成し、このD_iを開札装置１２に入力する。

開札装置１２は入力された全D_iを共有記録媒体２５に蓄積する（Ｓ４）。ま

た全D_iに対して、一方向性関数ｈ処理装置２２を用いて、$h^{f(n+1)-f(k)}$（D_i）を作成し（Ｓ５）、この$h^{f(n+1)-f(n)}$（D_i）が共有記録媒体２５上のC_iと各々一致するかを検証し（Ｓ６）、全て一致したならば、全てのD_iは正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【００３０】

ステップＳ６で全てが一致すれば一方向性関数ｇ処理装置２３を用いて、ｇ（D_i）を生成し（Ｓ７）、その各ｇ（D_i）が共有記録媒体２５上の入札データ中の入札指標γ_iに一致するかを検証する（Ｓ８）、一致するものが１つもなければ、共有記録媒体２５上のC_iをD_iで上書き（$C_i \leftarrow D_i$）し（Ｓ９）、減算器２４によりｋ←ｋ－１としてステップＳ３に戻る（Ｓ１０）。ステップＳ８で一致するものがあればその時のｋを落札価格とし、そのｋと、この落札価格を提示した入札装置11_iの識別子ID_iを出力する（Ｓ１１）。

【００３１】

この場合は開札装置１２にも落札価格以外の入札価格が知られないことになる。

次にこの例において、最低価格を落札価格とする場合を述べる。図１４に開札装置の構成を示す。図１２との相違は減算器２４の代りに加算器３４が設けられている点である。

【００３２】

この開札装置１２は図１５に示すように動作する。まず開札装置に入力された複数の入札データ（入札指標$\gamma_i = g(h^{f(n,PRi)}(IV_i))$、識別子$ID_i$）が共有記録媒体２５に蓄積される（Ｓ１）。また全入札装置と共有されている$h^{f(n,q-1)}(IV_i)$は予めC_iとして共有記録媒体２５に蓄積されている。ここではｍ個の入札があったとし、ｉ＝１，２，…，ｍとする。カウンタｋに下限値ｑをセットする（Ｓ２）。

【００３３】

全入札装置11_iに$h^{f(n,k)}(IV_i)$の提示を要求する（Ｓ３）。各入札装置11_iは各々の初期値IV_iを用いて$h^{f(n,k)}(IV_i)$（＝D_i）を生成し、このD_iを開札装置１２に入力する。

開札装置１２は入力された全D_iを共有記録媒体２５に蓄積する（Ｓ１５）。また全D_iに対して、一方向性関数ｈ処理装置２２を用いて、$h^{f(n,q-1)-f(n,k)}$（D_i）を作成し（Ｓ５）、これが共有記録媒体２５上のC_iと各々一致するかを検証する（Ｓ６）。その検証で全て一致したならば、全てのD_iは正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【００３４】

ステップＳ６で全て一致したならば一方向性関数ｇ処理装置２３を用いて、ｇ（D_i）を生成し（Ｓ７）、各ｇ（D_i）が共有記録媒体２５上の入札データ中の入札指標γ_iに一致するかを検証する。一致するものが１つもなければ、共有記録媒体２５上のC_iをD_iで上書き（$C_i \leftarrow D_i$）し（Ｓ９）、加算器１４によりｋ←ｋ＋１としてステップＳ３に戻る（Ｓ１０）。ステップＳ８で一致するものがあればその時のｋを落札価格とし、そのｋと、この落札価格を提示した入札装置の識別子ID_iを出力する（Ｓ１１）。

実施例３

この実施例３では開札装置１２は初期値IV_iを知る必要がなく、落札価格以外の入札価格が知られず、しかも通信を簡単にする。

【００３５】

まず最大値を落札価格とする場合について述べる。

開札装置１２は図１６に示すように図１２に対し、関数ｆ処理装置２６が設けられている点が異なる。

この装置の動作は図１７に示すように、まず開札装置に入力された複数の入札データ（入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$、識別子$ID_i$）が共有記録媒体２５に蓄積される（Ｓ１）。また全入札装置11_iと共有されている$h^{f(n+1)}(IV_i)$は予めC_iとして共有記録媒体２５に蓄積されている。ここではｍ個の入札があったとし、ｉ＝１，２，…，ｍとする。カウンタの計数値ｋを上限値ｎにセットする（Ｓ２）。

【００３６】

全入札装置11_iに価格ｋで入札したかどうか尋ねる（Ｓ３）。価格ｋで入札したという入札装置が１つもなければ（Ｓ４）、減算器２４によりｋ←ｋ－１と

してステップＳ３に戻る（Ｓ５）。

ステップＳ４で価格ｋで入札したという入札装置があれば、全入札装置11_iに$h^{f(k)}$（IV_i）の提示を要求する（Ｓ６）。各入札装置11_iは各々の初期値IV_iを用いて$h^{f(k)}$（IV_i）（＝D_i）を生成し、このD_iを開札装置１２に入力する。

【００３７】

開札装置１２は入力された全D_iを共有記録媒体２５に蓄積する（Ｓ７）。また全D_iに対して、一方向性関数ｈ処理装置２２を用いて、$h^{f(n+1)-f(k)}$（D_i）を作成し（Ｓ８）、これが共有記録媒体２５上のC_iと各々一致するかを検証し（Ｓ９）、全て一致したならば、全てのD_iは正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【００３８】

ステップＳ９で全て一定ならばまず、入札したという入札装置11_jが提示したD_jに対し、一方向性関数ｇ処理装置２３を用いて、ｇ（D_j）を生成し（Ｓ１０）、ｇ（D_j）が共有記録媒体２５上の入札装置11_jの入札データ中の入札指標γ_jに一致するかどうかを検証する（Ｓ１１）。一致すれば、確かに入札装置11_jは価格ｋで入札したと判断する。一致しなければエラーを返して終了する。

【００３９】

必要に応じて、次に他の（11_j以外の）入札装置11_iが、価格ｋ以上で入札していなかったかどうかを、次のように検証する。

$k \leq t \leq n$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$，$i \neq j$）に対して、ｇ（$h^{f(t)-f(k)}$（$h^{f(k)}$（IV_i））が共有記録媒体２５上の入札指標γ_iと一致するかを検証し（Ｓ１２）、一致するものがあれば、エラーを返して終了する。一致するものが１つもなければ、落札価格ｋと、この落札価格を提示した入札装置の識別子ID_iを出力する（Ｓ１３）。

【００４０】

この検証を行えば、例えばｋで入札したかの問い合せに対して入札したとの応答をしそこなった場合が救済される。この検証を行わない場合はステップＳ１１

でｋで入札したと判断した時にｋとＩＤ$_i$ を出力する。

このようにして開札装置１２にも落札価格以外の入札価格が知れずに、かつ通信量を削減することができる。

【００４１】

次にこの実施例３において最低価格を落札価格とする場合を説明する。

開札装置１２は図１８に示すように図１６に対し、減算器２４の代りに加算器３４が用いられる点が相違する。この装置の動作を図１９に示す。まず開札装置１２に入力された複数の入札データ（入札指標γ_i ＝ｇ（$h^{f(n,PRi)}$（ＩＶ$_i$））、識別子ＩＤ$_i$）が共有記録媒体２５に蓄積される（Ｓ１）。また全入札装置と共有されている$h^{f(n,q-1)}$（ＩＶ$_i$）は予めＣ$_i$ として記録媒体２５に蓄積されている。ここではｍ個の入札があったとし、ｉ＝１，２，…，ｍとする。カウンタの計数値ｋに下限値ｑをセットする（Ｓ２）。

【００４２】

全入札装置１１$_i$ に価格ｋで入札したかどうか尋ねる（Ｓ３）。価格ｋで入札したという入札装置が１つもなければ（Ｓ４）、加算器３４によりｋ←ｋ＋１としてステップＳ３に戻る（Ｓ５）。

価格ｋで入札したという入札装置があれば、全入札装置$h^{f(n,k)}$（ＩＶ$_i$）の提示を要求する（Ｓ６）。各入札装置１１$_i$ は各々の初期値ＩＶ$_i$ を用いて$h^{f(n,k)}$（ＩＶ$_i$）（＝Ｄ$_i$）を生成し、このＤ$_i$ を開札装置１２に入力する。

【００４３】

開札装置１２は入力された全Ｄ$_i$ を共有記録媒体２５に蓄積する（Ｓ７）。また全Ｄ$_i$ に対して、一方向性関数ｈ処理装置２２を用いて、$h^{f(n,q-1)-f(n,k)}$（Ｄ$_i$）を作成し（Ｓ８）、これが共有記録媒体２５上のＣ$_i$ と各々一致するかを検証し（Ｓ９）、全て一致したならば、全てのＤ$_i$ は正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【００４４】

ステップＳ９で全て一致すれば、入札したという入札装置１１$_j$ が提示したＤ$_j$ に対し、一方向性関数ｇ処理装置２３を用いて、ｇ（Ｄ$_j$）を生成し（Ｓ１０）、ｇ（Ｄ$_j$）が共有記録媒体２５上の入札装置１１$_j$ の入札データ中の入札指

標γ_jに一致するかどうかを検証する（Ｓ１１）。一致すれば、確かに入札装置11_jは価格ｋで入札したと判断する。一致しなければエラーを返して終了する。

【００４５】

必要に応じて次に他の（11_j以外の）入札装置11_iが、価格ｋ以下で入札していなかったかどうかを、次のように検証する。

$q \leq t \leq k$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$，$i \neq j$）に対して、$g(h^{f(n,t)-f(n,h)}(h^{f(n,k)}(IV_i)))$が共有記録媒体２５上の入札指標$\gamma_i$と一致するかを検証し、一致するものがあれば、エラーを返して終了する。一致するものが１つもなければ、落札価格ｋと、この落札価格を提示した入札装置11_iの識別子ID_iを出力する（Ｓ１３）。

【００４６】

落札装置にも落札価格以外の入札価格が知れずに、かつ通信量を削減し、最低入札価格を落札価格として求めることができる。

実施例４

この実施例４は開札装置１２における処理を簡単にし、かつ通信量を削減することを可能としたものである。

【００４７】

図２０に示すように各入札装置11_iはその入札装置11_iのみが知る乱数R_iを乱数生成装置１８で生成し、そのR_iと入札価格PR_iを用い演算装置１９でビット連結、加算、乗算などの適当な演算（これを（＋）で表わす）を行い、その結果に対し、一方向性関数ｈ処理を行い、その結果$h(PR_i (+) R_i)$を入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$と識別子$ID_i$と共に開札装置１２へ送る。

【００４８】

この場合の開札装置１２の機能構成を図２１に示し、その動作の流れを図２２に示す。各入札装置11_iごとに、$\gamma_i = g(h^{(PRi)}(IV_i))$、$h(PR_i (+) R_i)$，$ID_i$を入力として受け付け、共有記録媒体２５に蓄積する（Ｓ１）。また全入札装置11_iと共有されている$h^{f(n+1)}(IV_i)$は予めC_i

として共有記録媒体２５に蓄積されている。

【００４９】

全入力が揃うと、全入札装置11_iに入札価格PR_iと乱数R_iの提示を要求する（Ｓ２）。各入札装置11_iは各々PR_iとR_iを開札装置１２に入力し（Ｓ３）、この時点で開札装置１２には全入札価格が分かり、開札装置１２は最高値をｋとおき、ｋを入札した入札装置（落札装置）を11_jとする（Ｓ４）。なおこのPR_iの提示前は各入札装置は他の入札装置の入札価格を知ることはできない。

【００５０】

開札装置１２は全入札装置11_iに$h^{f(k)}(IV_i)$の提示を要求する（Ｓ５）。各入札装置11_iは各々の初期値IV_iを用いて$h^{f(k)}(IV_i)$（$=D_i$）を生成し、このD_iを開札装置１２に入力し、開札装置１２は入力された全D_iを共有記録媒体２５に蓄積する（Ｓ６）。また全D_iに対して、一方向性関数ｈ処理装置２２を用いて、$h^{f(n+1)-f(k)}(D_i)$を作成し（Ｓ７）、これが共有記録媒体２５上のC_iと各々一致するかを検証（Ｓ８）。全て一致したならば、全てのD_iは正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。なお、関数ｆ処理装置２６にｎ＋１とｋを入力してｆ（ｋ）、ｆ（ｎ＋１）を生成し、減算器３７でｆ（ｎ＋１）－ｆ（ｈ）を作って一方向性関数ｈ処理装置２２へ入力する。

【００５１】

ステップＳ８で全てが一致すれば、まず、落札装置11_jが提示したD_jに対し、一方向性関数ｇ処理装置２３を用いて、ｇ（D_j）を生成し（Ｓ９）、ｇ（D_j）が共有記録媒体２５上の11_jの入札データ中の入札指標γ_jに一致するかどうか検証する（Ｓ１０）。一致すれば、確かに入札装置11_jは価格ｋで入札したと判断する。一致しなければエラーを返して終了する。

【００５２】

必要に応じて次に他の（11_j以外の）入札装置11_iが、価格ｋ以上で入札していなかったかどうかを、次のように検証する。

$k \leq t \leq n$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$，$i \neq j$）に対して、

ｇ（$h^{f(t)-f(k)}$（$h^{f(k)}$（ＩＶ$_i$））が共有記録媒体２５上の入札指標γ_iと一致するかを検証し（Ｓ１１）、一致するものがあれば、エラーを返して終了する。一致するものが１つもなければ、落札価格ｋと、この落札価格を提示した入札装置１１$_i$の識別子ＩＤ$_i$を出力する（Ｓ１２）。なおｇ（$h^{f(t)-f(k)}$（$h^{f(k)}$（ＩＶ$_i$））の演算は制御装置２１″、関数ｆ処理装置２６′、一方向性関数ｈ処理装置２２′、一方向性関数ｇ処理装置２３で行う。

【００５３】

仮りにｉがｈ（ＰＲ′（＋）Ｒ$_i$）とγ_i＝ｇ（$h^{f(PRi)}$（ＩＶ$_i$）（ＰＲ$_i$′＞ＰＲ$_i$）を出力し、ＰＲ$_i$とＲ$_i$の提示要求に対し、ＰＲ′を提示し、これが最高値となった場合に、$h^{f(k)}$（ＩＶ$_i$）の提示要求に対し、$h^{f(PRi)}$（ＩＶ$_i$）を提示すると、ＰＲ$_i$′より低いＰＲ$_i$で落札してしまうおそれがあるが、ステップＳ１１の検証によりこのような悪為は防止できる。

【００５４】

開札装置１２は、落札価格およびこれを提示した入札装置をＰＲ$_i$とＲ$_i$から簡単に特定でき、かつ通信量を削減することができ、ＰＲ$_i$、Ｒ$_i$から決定した落札価格と入札装置が真のものであるかを検証することができる。

次にこの実施例４で最低入札価格を落札価格とする場合の開札装置１２における処理手順を図２３を参照して説明する。この場合各入札装置１１$_i$ごとに、γ_i＝ｇ（$h^{f(n,PRi)}$（ＩＶ$_i$））とｈ（ＰＲ$_i$（＋）Ｒ$_i$）とＩＤ$_i$を入力として受け付け、記録媒体２５に記録する（Ｓ１）、また全入札装置１１$_i$と共有されている$h^{f(n,q-1)}$（ＩＶ$_i$）は予めＣ$_i$として共有記録媒体２５に蓄積されている。

【００５５】

全入力が揃うと、全入札装置１１$_i$に入札価格ＰＲ$_i$と乱数Ｒ$_i$の提示を要求する（Ｓ２）。各入札装置１１$_i$は各々ＰＲ$_i$とＲ$_i$を開札装置１２に入力し（Ｓ３）、この時点で開札装置１２には全入札価格ＰＲ$_i$が分かり、開札装置１２はその最低値をｋとおき、ｋを入札した入札装置（落札装置）を１１$_j$とする（Ｓ４）。

【００５６】

開札装置１２は全入札装置11_iに$h^{f(n,k)}$（IV_i）の提示を要求する（Ｓ５）。各入札装置11_iは各々の初期値IV_iを用いて$h^{f(n,k)}$（IV_i）（＝D_i）を生成し、このD_iを開札装置１２に入力。開札装置１２は入力された全D_iを共有記録媒体２５に蓄積する（Ｓ６）。また全D_iに対して、一方向性関数ｈ処理装置を用いて、$h^{f(n,q-1)-(n,k)}$（D_i）を作成し（Ｓ７）、これが共有記録媒体２５上のC_iと各々一致するかを検証し（Ｓ８）、全て一致したならば、全てのD_iは正しいとし、以下を続行する。なお、正しくなければエラーを返して終了する。

【００５７】

ステップＳ８で全て一致するならばまず、落札装置11_jが提示したD_jに対し、一方向性関数ｇ処理装置を用いて、ｇ（D_j）を生成し（Ｓ９）、ｇ（D_j）が共有記録媒体上の落札装置11_jの入札データ中の入札指標γ_jに一致するかどうか検証する（Ｓ１０）。一致すれば、確かに11_jは価格ｋで入札したと判断する。一致しなければエラーを返して終了する。

【００５８】

必要に応じて次に他の（11_j以外の）入札装置11_iが、価格ｋ以下で入札していなかったかどうかを、次のように検証する。

$q \leq t \leq k$であるｔと、ｊを除く全てのｉ（$1 \leq i \leq m$，$i \neq j$）に対して、ｇ（$h^{f(n,t)-f(n,k)}$（$h^{f(n,k)}$（IV_i））が共有記録媒体２５上の入札指標γ_iと一致するかを検証し（Ｓ１１）、一致するものがあれば、エラーを返して終了する。一致するものが１つもなければ、落札価格ｋと、この落札価格を提示した入札装置11_iの識別子ID_iを出力する（Ｓ１２）。

【００５９】

この最低入札価格を落札価格とし、それが真であることを検証することができる。

実施例４において各入札装置11_iからｈ（PR_i（＋）R_i）も出力するようにしたが、ｈ（PR_i（＋）R_i）の代りにｈ（PR_i（＋）l_i（＋）R_i）を出力するようにしてもよい。ただし、l_iは入札者ｉが示すこの入札に関する付加情報であり、納品可能商品個数などである。この場合の開札処理は図２２

、図２３に示した場合とほぼ同様であるが、全ての入札装置から入札データγ_i、ID_i、h（PR_i（＋）l_i（＋）R_i）を受け取った後に、全入札装置11_iに対し、PR_i、l_i、R_iの提示を要求する点が異なるだけである。

実施例５

この実施例５は入札可能なｎ種類の価格について全てを含む入札指標を送出する。図２４に示すように入札装置11_iの入札価格変換装置１４は、制御装置４１、乱数生成装置４２、一方向性関数ｈ処理装置４３、関数ｆ処理装置４４、$b_i^{(j)}$、生成装置４５、（＋）演算装置４６、加算器４７から成る。関数ｆ処理装置４１は図５中の関数ｆ処理装置１５と同様のものである。

【００６０】

入札可能なｎ種類の価格１，２，…，ｎのうち、入札装置11_iが実際に入札しようとしている価格をPR_iとする。また、入札装置11_iにおいて、$1 \leq j \leq n$なるｊに対して、価格ｊを入札しない場合は$b^{(i)}=0$、価格ｊを入札する場合は$b^{(j)}=1$と$b^{(j)}$を定義する。従って$1 \leq j \leq n$なるｊに対して、$b^{(j)}$は唯１つのみ１である。$R_i^{(j)}$を入札装置11_iしか知らずｊごとに異なる乱数として、全ての入札可能価格に対し、入札装置11_iは{ID_i，h（f（1）（＋）$b_i^{(1)}$（＋）$R_i^{(1)}$），h（f（２）（＋）$b_i^{(2)}$（＋）$R_i^{(2)}$），…，h（f（ｎ）（＋）$b_i^{(n)}$（＋）$R_i^{(n)}$）}を出力する。

【００６１】

図２５を参照して、このｎ個からなる入札指標の生成手順を説明する。入札価格PR_iが決定入力され（Ｓ１）、価格パラメータｊを１とし（Ｓ２）、$j \leq n$か否かを調べ（Ｓ３）、$j \leq n$であれば、関数ｆ処理装置４４にｊを入力してｆ（ｊ）を生成し（Ｓ４）、また乱数生成装置４２から乱数$R_i^{(j)}$を生成し（Ｓ５）、更に$b_i^{(j)}$生成装置４５から入札価格PR_iに応じて価格選択有無情報$b_i^{(j)}$を生成する（Ｓ６）。（＋）演算装置４６はこれらｆ（ｊ）、$R_i^{(j)}$，$b_i^{(j)}$を入力してｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$を演算する（Ｓ７）。（＋）は適当の演算を示す。この演算結果を一方向性関数ｈ処理装置４３で処理してｈ（ｆ（ｊ）（＋）$b_i^{(j)}$（＋）$R_i^{(j)}$）を生成する（Ｓ８）。次にｊを＋１してステップＳ３に戻る（Ｓ９）。ｊがｎを換え、全てのｊについて

の処理が終ると、入札装置11_iから識別子ID_iと、入札指標｛h（f（1）（+）$b_i^{(1)}$（+）$R_i^{(1)}$），…，h（f（n）（+）$b_i^{(n)}$（+）$R_i^{(n)}$）｝を出力する（Ｓ１０）。

【００６２】

このように一方向性関数を用いて各価格に対する入札指標を作成し、全指標を出力することにより、本命の入札価格を秘密にできることができる。

このような入札データを入力して開札処理を行う開札装置１２は図２６に示すように制御装置２１、一方向性関数ｈ処理装置２２、関数ｆ処理装置２６、減算器２４、メモリ手段３５、および他の装置からも参照可能な共有記録媒体２５、（＋）演算装置５１から成る。

【００６３】

この開札装置１２の動作は図２７に示すように、$1 \leq i \leq m$というｉに対して、｛ID_i，h（f（1）（+）$b_i^{(1)}$（+）$R_i^{(1)}$），h（f（2）（+）$b_i^{(2)}$（+）$R_i^{(2)}$），…，h（f（n）（+）$b_i^{(n)}$（+）$R_i^{(n)}$）｝が入力され、これらを共有記録媒体２５に蓄積する（Ｓ１）。価格パラメータｋをその最高値ｎとする（Ｓ２）。全入札装置11_iに$R_i^{(k)}$の提示を要求する（Ｓ３）。各入札装置11_iは各々$R_i^{(k)}$を開札装置１２に入力する。開札装置１２はその全ての$R_i^{(k)}$を共有記録媒体２５に蓄積する（Ｓ４）。開札装置１２は$b_i^{(k)}$＝１とし、関数ｆ処理装置２６でｆ（ｋ）を求め、このｆ（ｋ）と$b_i^{(k)}$＝１と$R_i^{(k)}$を（＋）演算装置５１に入力して、ｆ（ｋ）（+）１（+）$R_i^{(k)}$を演算し、その結果を一方向性関数ｈ処理装置２２で処理してｈ（ｆ（ｋ）（+）１（+）$R_i^{(k)}$）を求める。各ｉに対してｈ（ｆ（ｋ）（+）１（+）$R_i^{(k)}$）が共有記録媒体２５上にあるかどうかを検証する（Ｓ５）。もしなければｋ←ｋ－１としてステップＳ３に戻る（Ｓ６）。ステップＳ５で一致するものがあれば、そのｋを落札価格ｋとし、ｋと、この落札価格を提示した入札装置11_iの識別子ID_iを出力して終了する（Ｓ７）。

【００６４】

このように一方向性関数を用いて各価格に対する入札指標を作成し、かつ全指標を開札対象とし、最高値から順にオープンすることにより非落札価格を秘密に

できる。

この実施例５において最低入札価格を落札価格とする場合は、入札装置11_iから同様に｛ID_i，h（f（1）（+）$b_i^{(1)}$（+）$R_i^{(1)}$），h（f（2）（+）$b_i^{(2)}$（+）$R_i^{(2)}$），…，h（f（n）（+）$b_i^{(n)}$（+）$R_i^{(n)}$）｝を開札装置へ送る。開札装置１２では図２７に示した処理とほぼ同様に処理するが、ステップＳ２では入札可能なｎ種類の価格の最低値１をｋにセットし、ステップＳ６ではｋ←ｋ＋１とする。その他の処理は同様である。

【００６５】

この実施例５において最高価格を入札価格とする場合は$n \leq k' \leq k$なるｋ′について$R_i^{(k')}$が共有記録媒体２５に記録されているから、その落札価格ｋが正しいものであるかを、誰でもが調べることができる。

この実施例５において、乱数$R_i^{(j)}$が入札装置11_i自身の他に開札装置１２も知っているようにすることもできる。その場合の開札装置１２の処理を図２８に示す。

【００６６】

各入札装置11_iから、$1 \leq i \leq m$というｉに対して、｛ID_i，h（f（1）（+）$b_i^{(1)}$（+）$R_i^{(1)}$），h（f（2）（+）$b_i^{(2)}$（+）$R_i^{(2)}$），…，h（f（n）（+）$b_i^{(n)}$（+）$R_i^{(n)}$）｝が入力され、これらを共有記録媒体２５に蓄積する（Ｓ１）。価格パラメータｋを取り得る最高値ｎとする（Ｓ２）。開札装置１２は全てのｉに対して、$b_i^{(k)}$＝１としてｈ（f（k）（+）１（+）$R_i^{(k)}$）を作成し、この値が共有記録媒体２５上に一致するものが存在するかを検証する（Ｓ３）。一致するものがなければｋ←ｋ－１としてステップ３に戻る（Ｓ４）。一致するものがｋ′≧ｈである全ての$R_i^{(k')}$を共有記録媒体２５に蓄積し（Ｓ５）、この時のｋを落札価格とし、このｋと、この落札価格を提示した入札装置11_iの識別子ID_iを出力して終了する（Ｓ６）。

【００６７】

この場合で最低入札価格を落札価格とする場合は、図２８において、ステップＳ２で、ｋを、取り得る価格の最小値、この例では１とし、ステップＳ４ではｋ

を＋１とし、ステップＳ５ではｋ′≦ｋである全ての$R_i^{(k')}$を共有記録媒体２５に蓄積する。その他は図２８の処理と同様である。

仮識別子装置を用いた電子競争入札装置

図２９に仮識別子装置を用いた電子競争入札装置を示す。

【００６８】

各入札装置11_iは仮識別子登録装置５２と通信することができるようにされている。

この電子競争入札装置の動作は図３０に示すように行われる。

Ｓｔｅｐ１：入札装置11_iは外部から入力された入札公告を受けて、識別子ID_iを出力し、仮識別子登録装置５２へ入力する。

Ｓｔｅｐ２：仮識別子登録装置５２は入力されたID_iに対して、仮識別子であるAID_iを発行し、記録媒体５３にID_iとAID_iを組にして保存し、AID_iを入札装置11_iへ返す。

Ｓｔｅｐ３：入札装置11_iは入札価格PR_iを生成し、

Ｓｔｅｐ４：その入札価格を入札指標γ_iに変換し、

Ｓｔｅｐ５：入札装置11_iは入札指標γ_iとAID_iを出力し、開札装置１２へ入力する。

Ｓｔｅｐ６：開札装置１２は全入札指標から落札価格を求め、

Ｓｔｅｐ７：落札価格と、この落札価格を提示した入札装置の仮識別子を出力する。

【００６９】

このようにして誰れが入札へ参加したかを秘密にしておくことができる。なお開札装置１２は仮識別子登録装置５２に問い合わせて、落札価格と対応する仮識別子がAID_iから識別子ID_iを知ることができる。

上述においてｆ（PR_i）は単調増加かつ正整数を出力する関数であるが、ｆ（PR_i）＝PR_iも含むものである。ｆ（ｎ，PR_i）は例えばｎ－PR_iである。入札装置11_iや開札装置１２はその機能をコンピュータによりプログラムを解読実行させることにより作用させることもできる。

【００７０】

【発明の効果】

以上述べたようにこの発明によれば、入札価格を、一方向性関数を利用して入札指標に変換して、開札装置へ送っているため、入札前に各入札装置は他の入札装置の入札価格を知ることができず、公平に入札を行うことができる。

また$h^{f(n+1)}(IV_i)$や$h^{f(n,q'-1)}(IV_i)$を全入札装置間に共有させ、落札価格に対応する$h^{f(PRi)}(IV_i)$や$h^{f(n,PRi)}(IV_i)$を公開することにより、落札価格が確かに改ざんされることなく、正しくその額で入札されたものであるか否かを、全ての入札装置が検証することができる。

【００７１】

またこの発明によれば落札価格以外の入札価格を秘密にしたまま、落札価格を判定することができる。

実施例２によれば開札装置にも落札価格以外の入札価格が知れない。

実施例３によれば、開札装置にも落札価格以外の入札価格が知れず、しかも、入札装置との通信量を消滅することができる。

【００７２】

実施例４によれば、入札時には、入札価格が他に知られるおそれがなく、しかも開札時には、直接入札価格から落札価格を簡単に特定でき、かつその落札価格が正しいことを検証することができる。

実施例５によれば、一方向性関数により各価格に対する入札指標を作成し、その全ての指標を開札装置へ送ることにより、本命の入札価格を秘密にすることができる。

【図面の簡単な説明】

【図１】

電子競争入札装置の一般的構成を示すブロック図。

【図２】

電子競争入札の一般的手順を示す流れ図。

【図３】

入札指標を生成する入札装置を示すブロック図。

【図４】

一方向性関数により入札指標を生成する入札装置を示すブロック図。

【図５】

一方向性関数処理装置による入札価格変換装置の具体例を示すブロック図。

【図６】

一方向性関数により入札指標を生成する手順を示す流れ図。

【図７】

実施例１の最高入札価格を落札価格とする開札装置１２の機能構成を示すブロック図。

【図８】

図７の開札装置の動作を示す流れ図。

【図９】

実施例１の最低入札価格を落札価格とする場合の入札価格変換装置を示すブロック図。

【図１０】

実施例１の最低入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図１１】

図１０の開札装置の動作を示す流れ図。

【図１２】

実施例２の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図１３】

図１２の開札装置の動作手順を示す流れ図。

【図１４】

実施例２の最低入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図１５】

図１４の開札装置の動作手順を示す流れ図。

【図１６】

実施例３の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図１７】

図１６の開札装置の動作手順を示す流れ図。

【図１８】

実施例３の最低入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図１９】

図１８の開札装置の動作手順を示す流れ図。

【図２０】

実施例４の入札装置の例を示すブロック図。

【図２１】

実施例４の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図２２】

図２１の開札装置の動作手順を示す流れ図。

【図２３】

実施例４の最低入札価格を落札価格とする場合の開札装置の動作手順を示す流れ図。

【図２４】

実施例５の入札装置の機能構成を示すブロック図。

【図２５】

図２４の入札装置の動作手順を示す流れ図。

【図２６】

実施例５の最高入札価格を落札価格とする場合の開札装置の機能構成を示すブロック図。

【図２７】

図２６の開札装置の動作手順を示す流れ図。

【図２８】

実施例５の変形における開札装置の動作手順を示す流れ図。

【図２９】

仮識別子を用いた電子競争入札装置を示すブロック図。

【図３０】

図２９の装置の入札手順を示す流れ図。

【書類名】　図面

【図１】

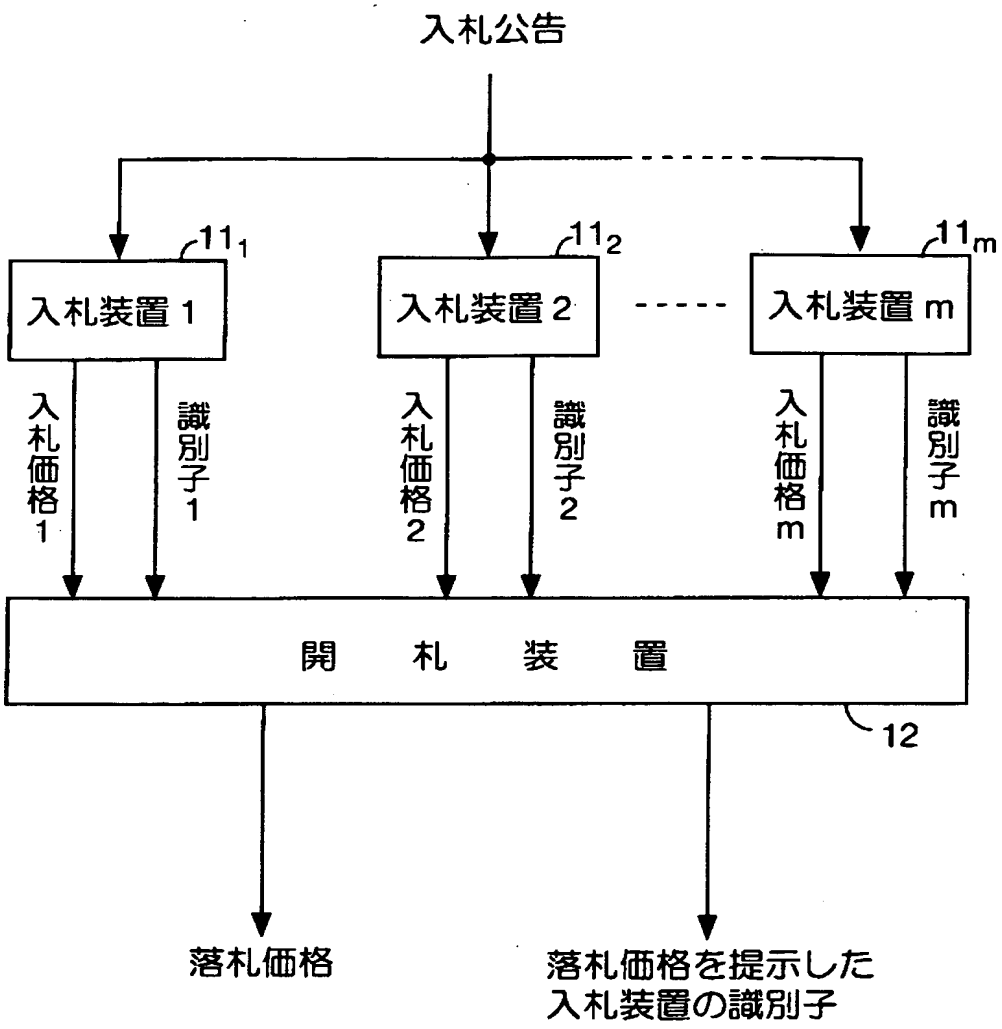

図１

出証特２０００－３０４６８３５

【図２】

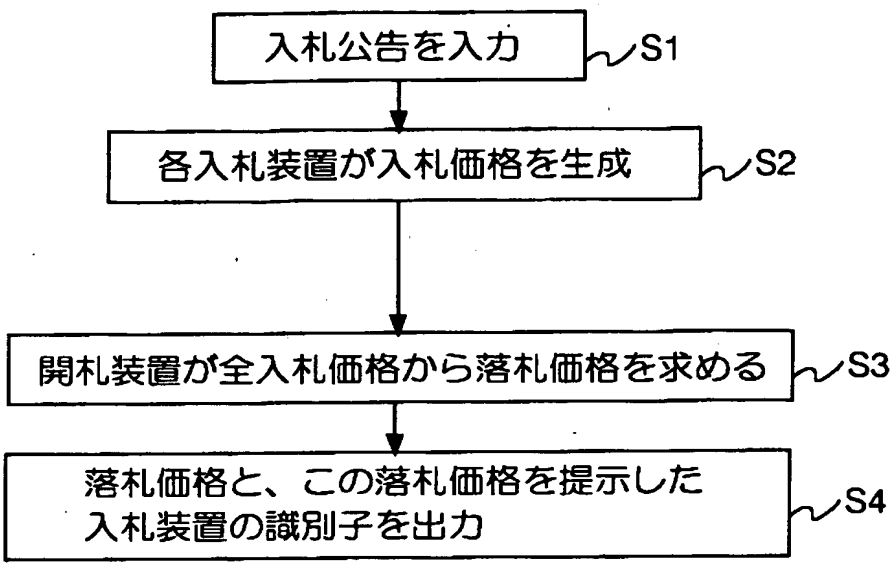
入札公告を入力
S1
各入札装置が入札価格を生成
S2
開札装置が全入札価格から落札価格を求める
S3
落札価格と、この落札価格を提示した
入札装置の識別子を出力
S4

図２

【図３】

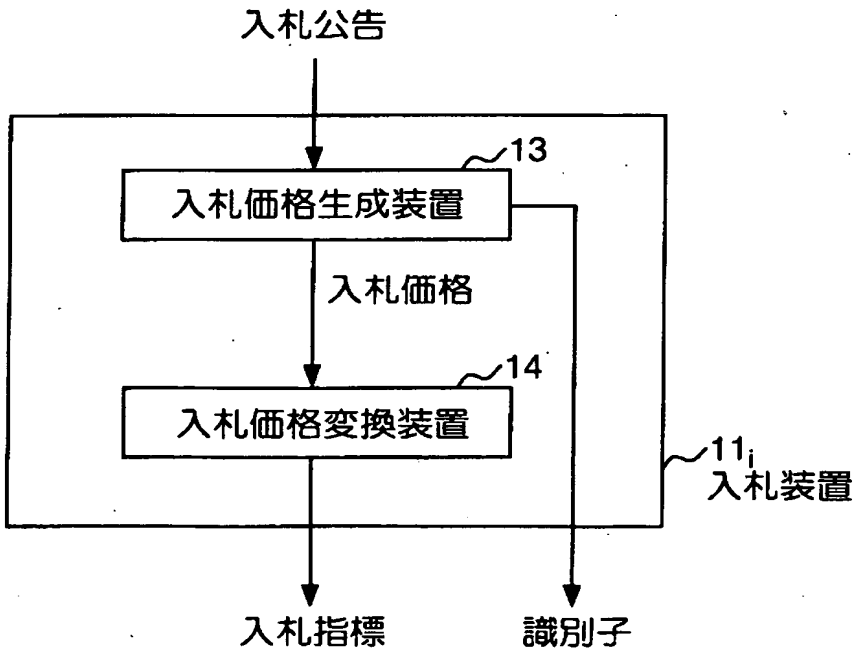
入札公告
13
入札価格生成装置
入札価格
14
入札価格変換装置
11i
入札装置
入札指標
識別子

図３

【図４】

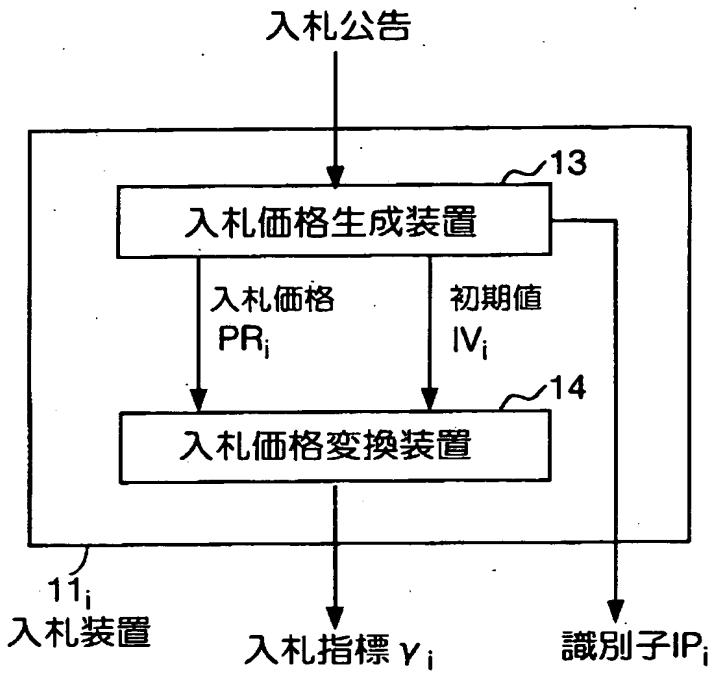
入札公告
13
入札価格生成装置
入札価格
PRi
初期値
IVi
14
入札価格変換装置
11i
入札装置
入札指標 γi
識別子IPi

図４

【図５】

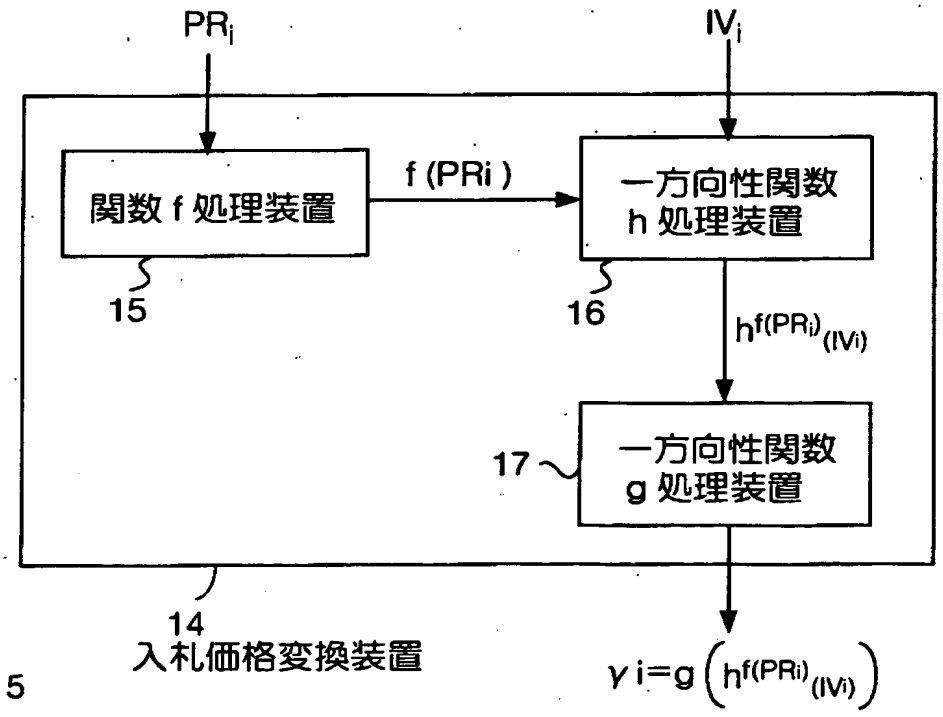
PRi
IVi
関数 f 処理装置
f (PRi)
一方向性関数
h 処理装置
15
16
h^f(PRi)(IVi)
17
一方向性関数
g 処理装置
14
入札価格変換装置
γi=g(h^f(PRi)(IVi))

図５

【図６】

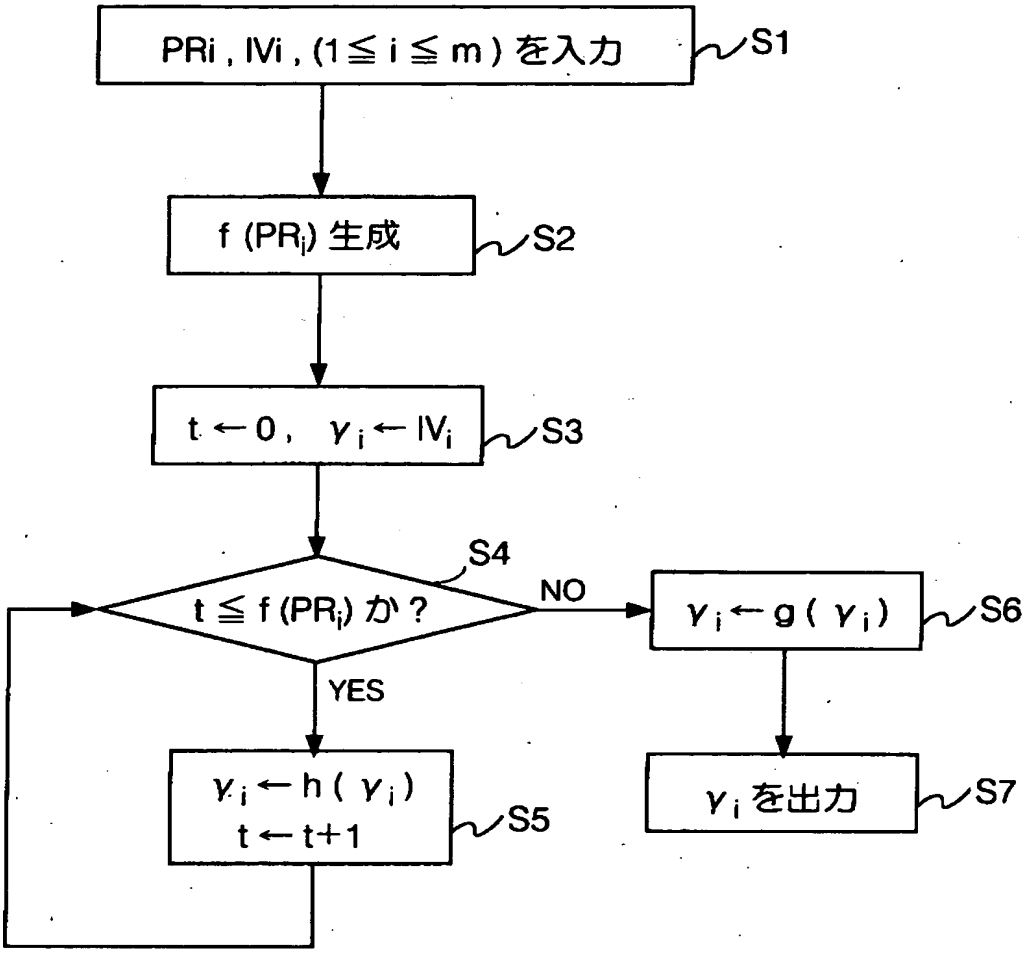
PRi , IVi , (1≦ i ≦ m) を入力
S1
f (PRi) 生成
S2
t ← 0 , γi ← IVi
S3
S4
t ≦ f (PRi) か？
NO
γi ← g (γi)
S6
YES
γi ← h (γi)
t ← t+1
S5
γi を出力
S7

図６

【図７】

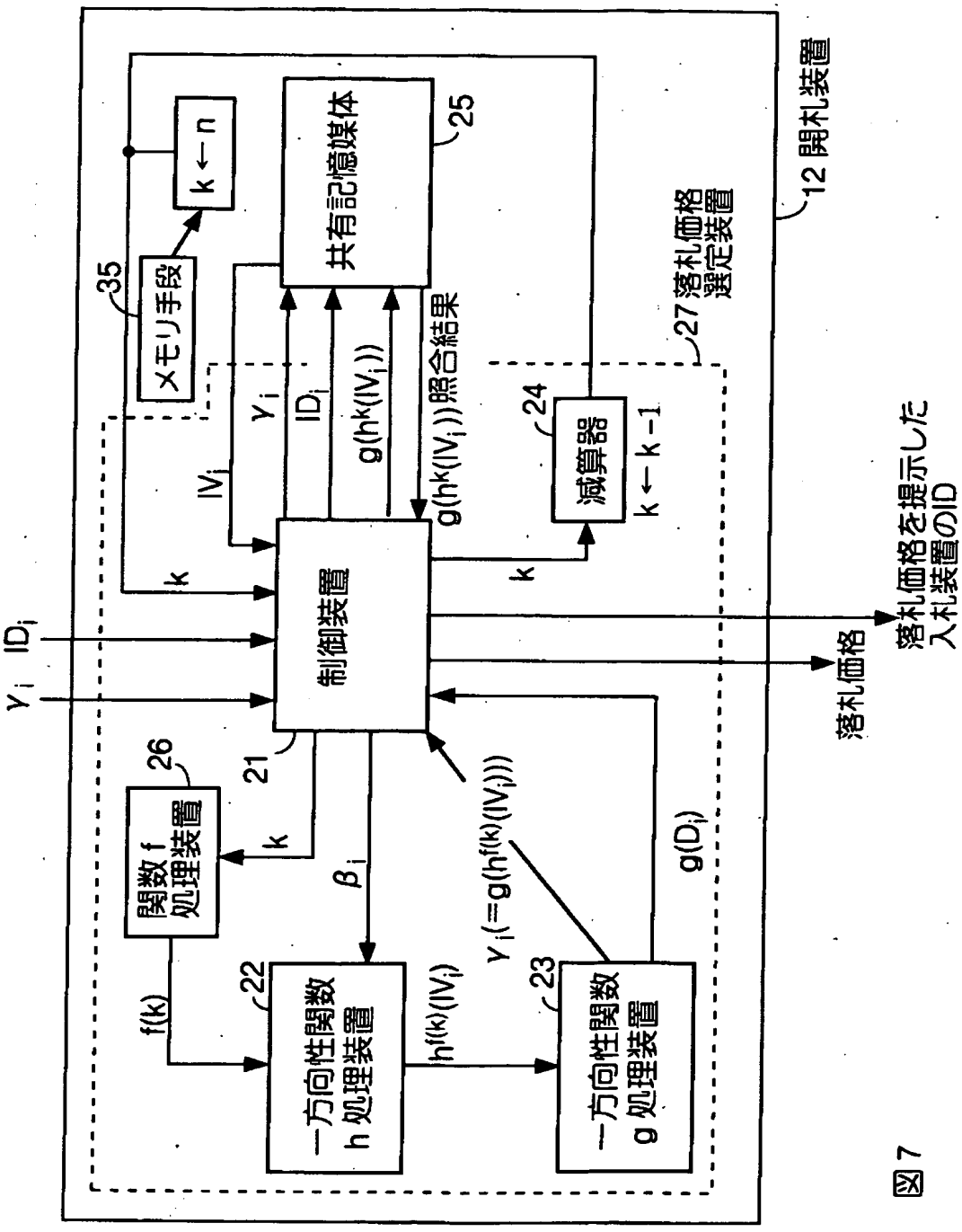
12 開札装置
27 落札価格選定装置
25
共有記憶媒体
k←n
35
メモリ手段
ID_i
γ_i
IV_i
$g(h^k(IV_i))$照合結果
24
減算器
k←k-1
k
制御装置
21
落札価格を提示した入札装置のID
落札価格
26
関数f処理装置
β_i
$\gamma_i(=g(h^{f(k)}(IV_i)))$
$g(D_i)$
f(k)
22
一方向性関数h処理装置
$h^{f(k)}(IV_i)$
23
一方向性関数g処理装置

図７

【図８】

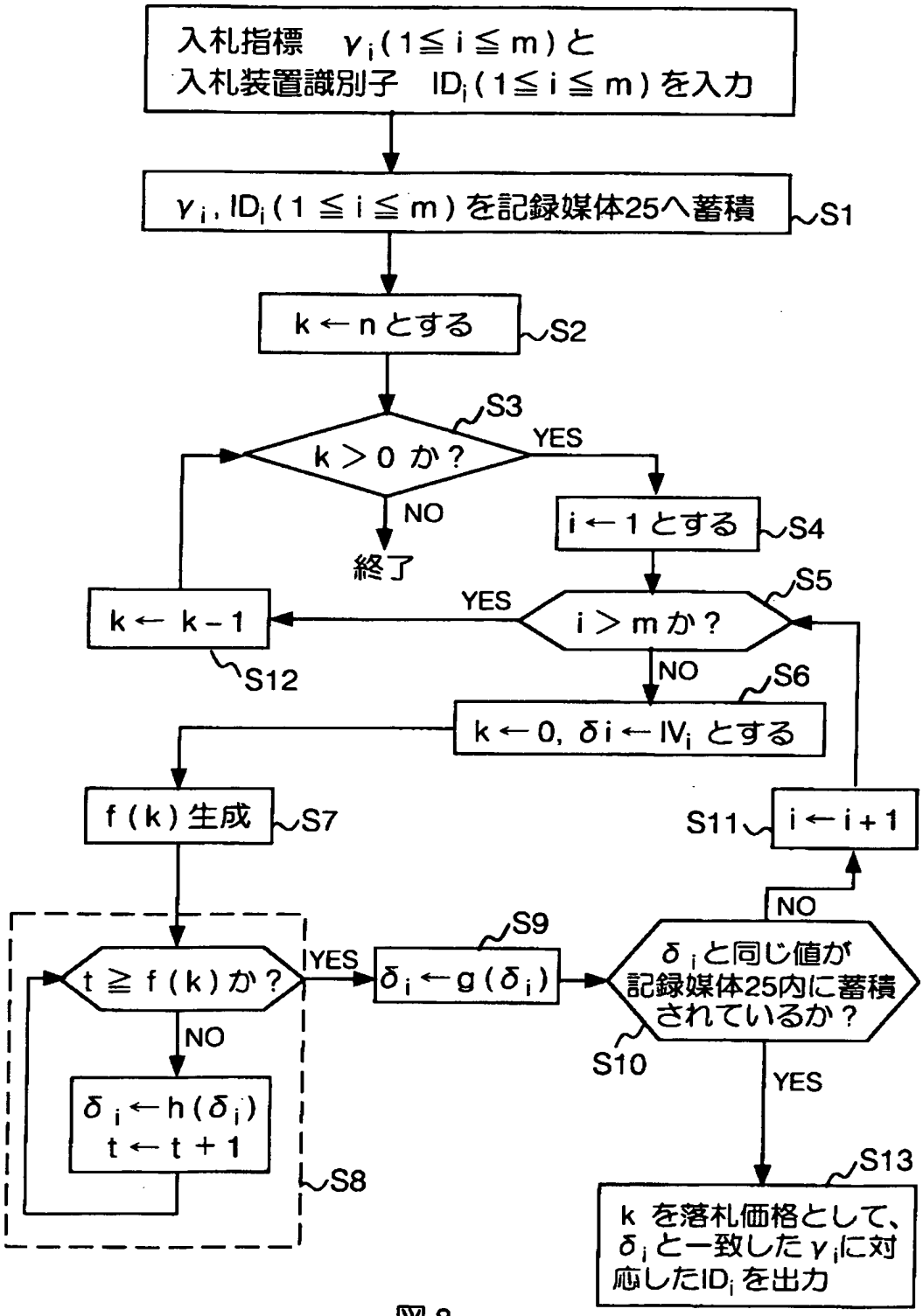
入札指標　γ_i ($1 \leqq i \leqq m$) と
入札装置識別子　ID_i ($1 \leqq i \leqq m$) を入力
γ_i, ID_i ($1 \leqq i \leqq m$) を記録媒体25へ蓄積
S1
k ← n とする
S2
S3
k > 0 か？
YES
NO
終了
i ← 1 とする
S4
S5
i > m か？
YES
k ← k − 1
S12
NO
S6
k ← 0, $\delta i \leftarrow IV_i$ とする
f (k) 生成
S7
S11
i ← i + 1
NO
S9
t ≧ f (k) か？
YES
$\delta_i \leftarrow g(\delta_i)$
δ_i と同じ値が
記録媒体25内に蓄積
されているか？
S10
NO
$\delta_i \leftarrow h(\delta_i)$
t ← t + 1
S8
YES
S13
k を落札価格として、
δ_i と一致した γ_i に対
応した ID_i を出力

図８

【図９】

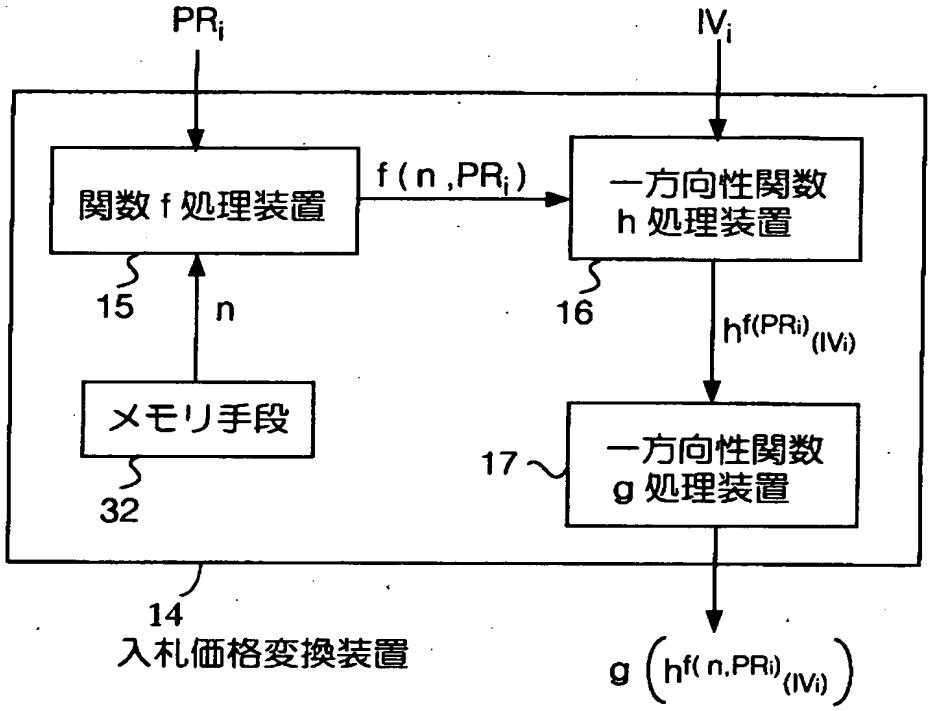
PRi
IVi
関数ｆ処理装置
f(n,PRi)
一方向性関数
h 処理装置
15
n
16
hf(PRi)(IVi)
メモリ手段
17
一方向性関数
g 処理装置
32
14
入札価格変換装置
g(hf(n,PRi)(IVi))

図９

【図１０】

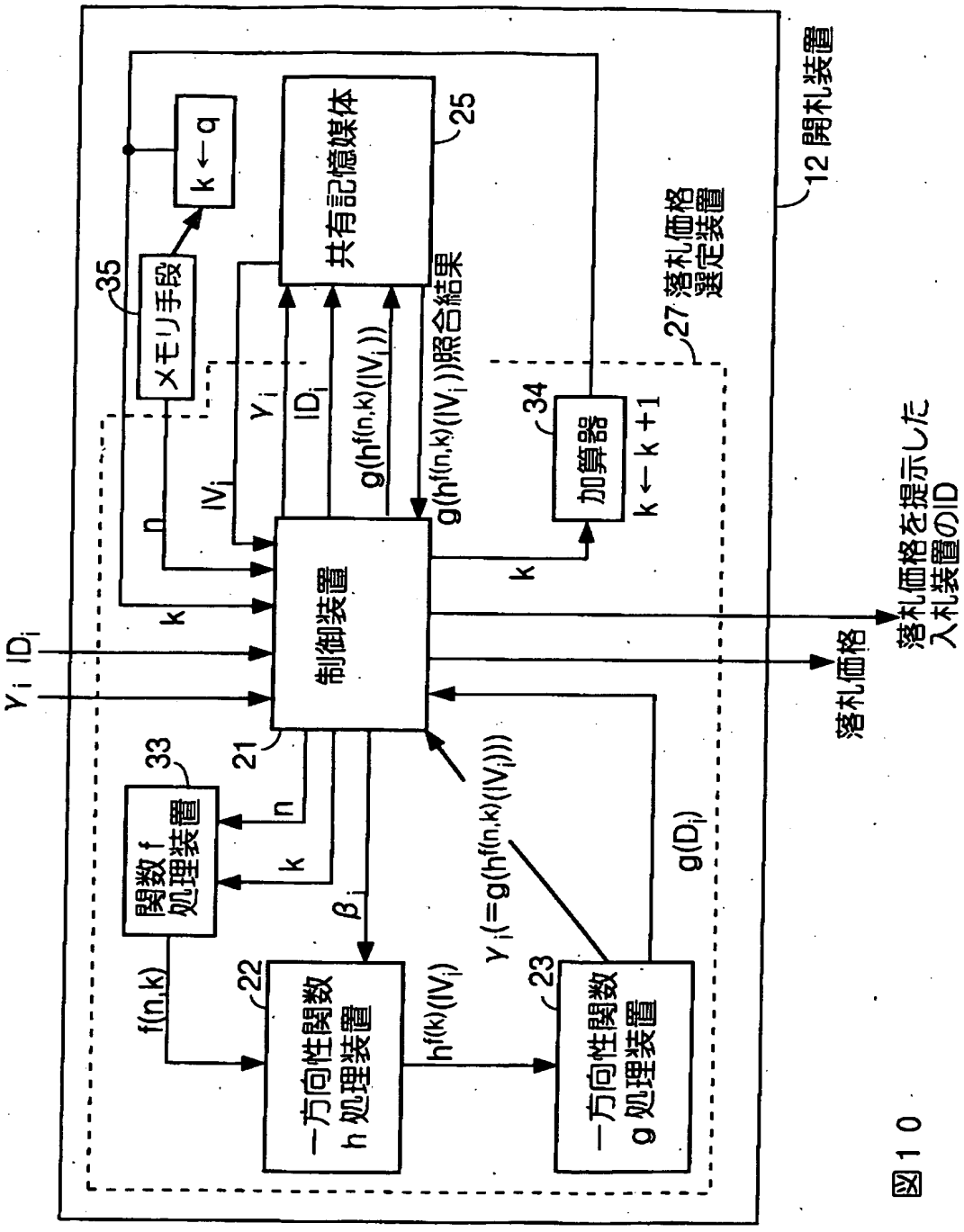
12 開札装置
27 落札価格選定装置
25 共有記憶媒体
35 メモリ手段
k←q
34 加算器
k←k+1
制御装置
21
33 関数f処理装置
22 一方向性関数h処理装置
23 一方向性関数g処理装置
落札価格を提示した入札装置のID
落札価格

図１０

【図１１】

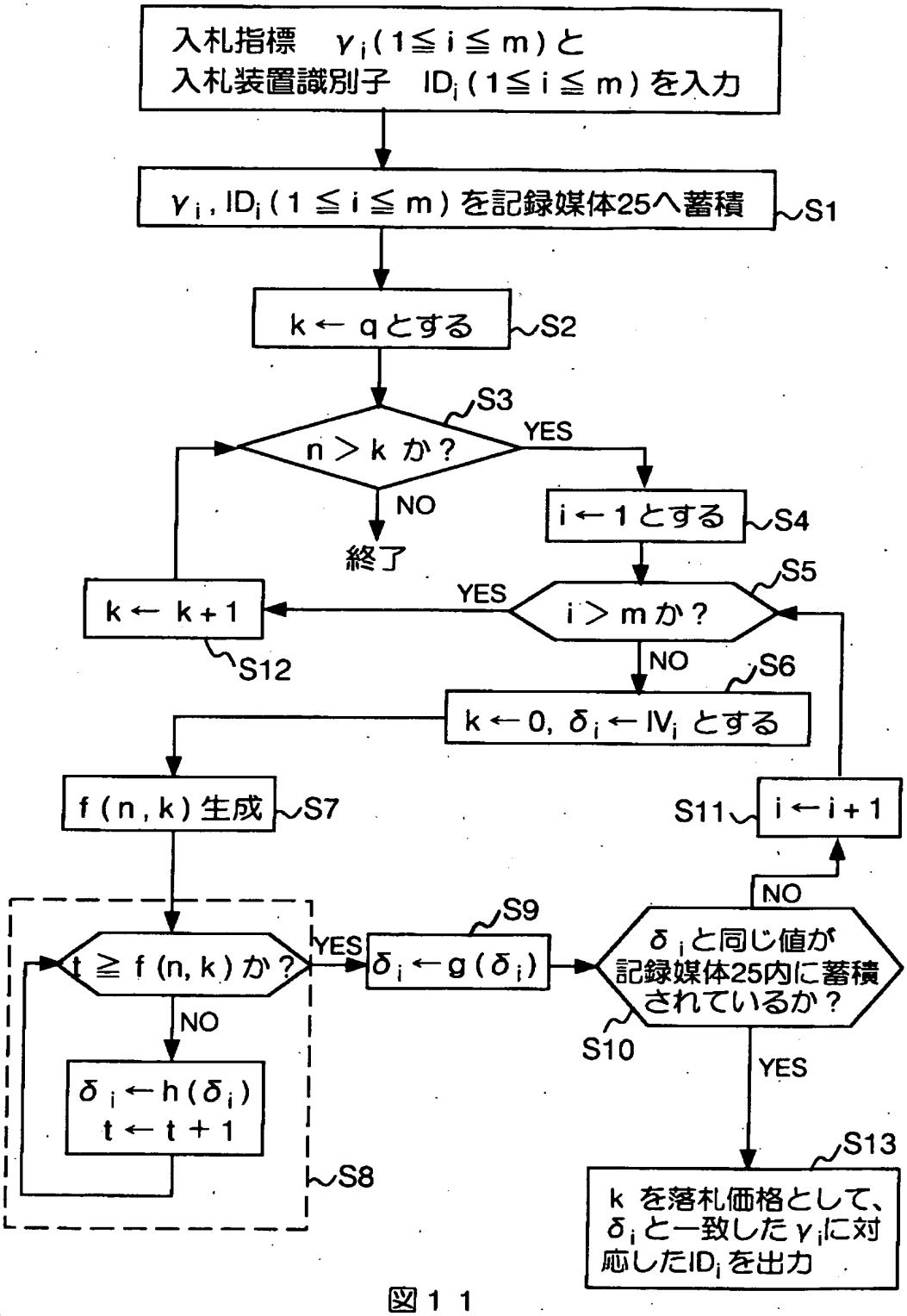
入札指標　γ_i ($1 \leqq i \leqq m$) と
入札装置識別子　ID_i ($1 \leqq i \leqq m$) を入力
γ_i , ID_i ($1 \leqq i \leqq m$) を記録媒体25へ蓄積
S1
k ← q とする
S2
S3
n > k か？
YES
NO
終了
i ← 1 とする
S4
S5
i > m か？
YES
k ← k + 1
S12
NO
S6
k ← 0, $\delta_i \leftarrow IV_i$ とする
f (n , k) 生成
S7
S11
i ← i + 1
NO
S9
t ≧ f (n, k) か？
YES
$\delta_i \leftarrow g(\delta_i)$
δ_i と同じ値が
記録媒体25内に蓄積
されているか？
S10
NO
$\delta_i \leftarrow h(\delta_i)$
t ← t + 1
S8
YES
S13
k を落札価格として、
δ_i と一致した γ_i に対
応した ID_i を出力

図１１

【図１２】

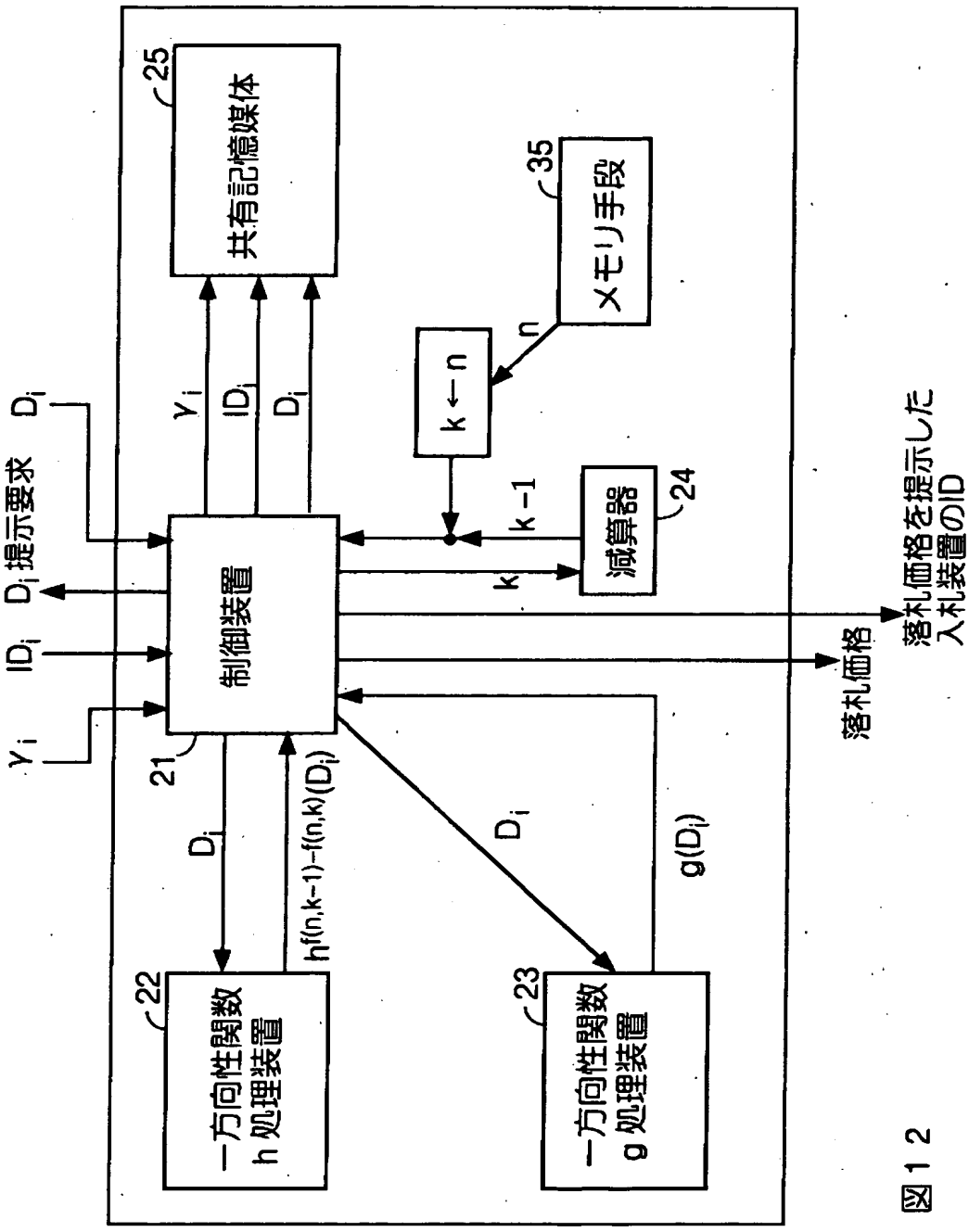
共有記憶媒体
25
メモリ手段
35
n
k←n
減算器
24
k
k-1
制御装置
21
D_i
ID_i
Y_i
D_i 提示要求
ID_i
Y_i
落札価格
落札価格を提示した
入札装置のID
D_i
$h^{f(n,k-1)-f(n,k)}(D_i)$
D_i
$g(D_i)$
一方向性関数
h 処理装置
22
一方向性関数
g 処理装置
23

図１２

【図１３】

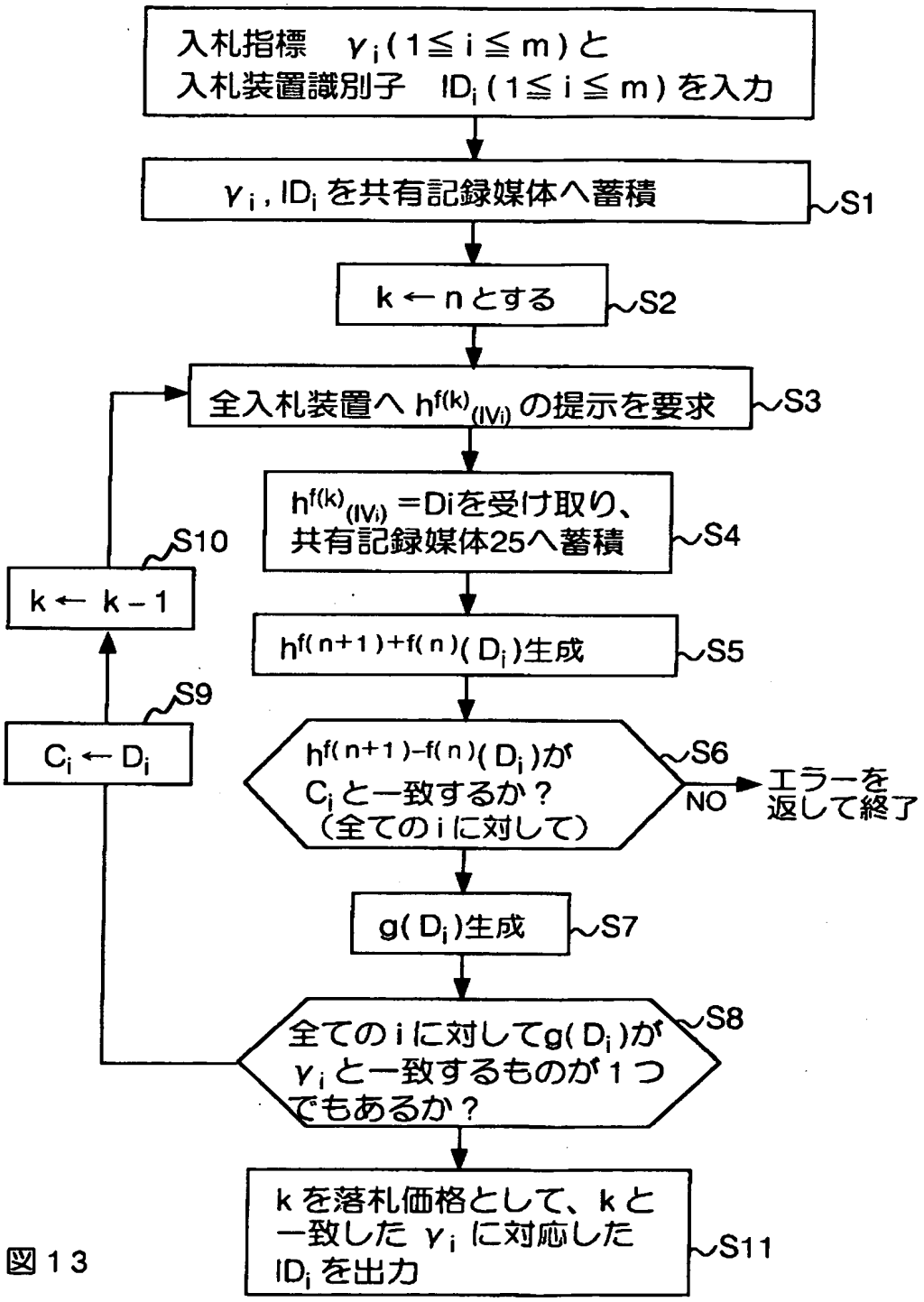
入札指標　γ_i (1≦ i ≦ m) と
入札装置識別子　ID_i (1≦ i ≦ m) を入力
γ_i , ID_i を共有記録媒体へ蓄積
S1
k ← n とする
S2
全入札装置へ $h^{f(k)}_{(IVi)}$ の提示を要求
S3
$h^{f(k)}_{(IVi)}$ =Diを受け取り、
共有記録媒体25へ蓄積
S4
$h^{f(n+1)+f(n)}(D_i)$生成
S5
$h^{f(n+1)-f(n)}(D_i)$が
C_iと一致するか？
（全てのiに対して）
S6
NO
エラーを
返して終了
g(D_i)生成
S7
全てのiに対してg(D_i)が
γ_i と一致するものが１つ
でもあるか？
S8
k を落札価格として、k と
一致した γ_i に対応した
ID_i を出力
S11
k ← k－1
S10
C_i ← D_i
S9

図１３

【図１４】

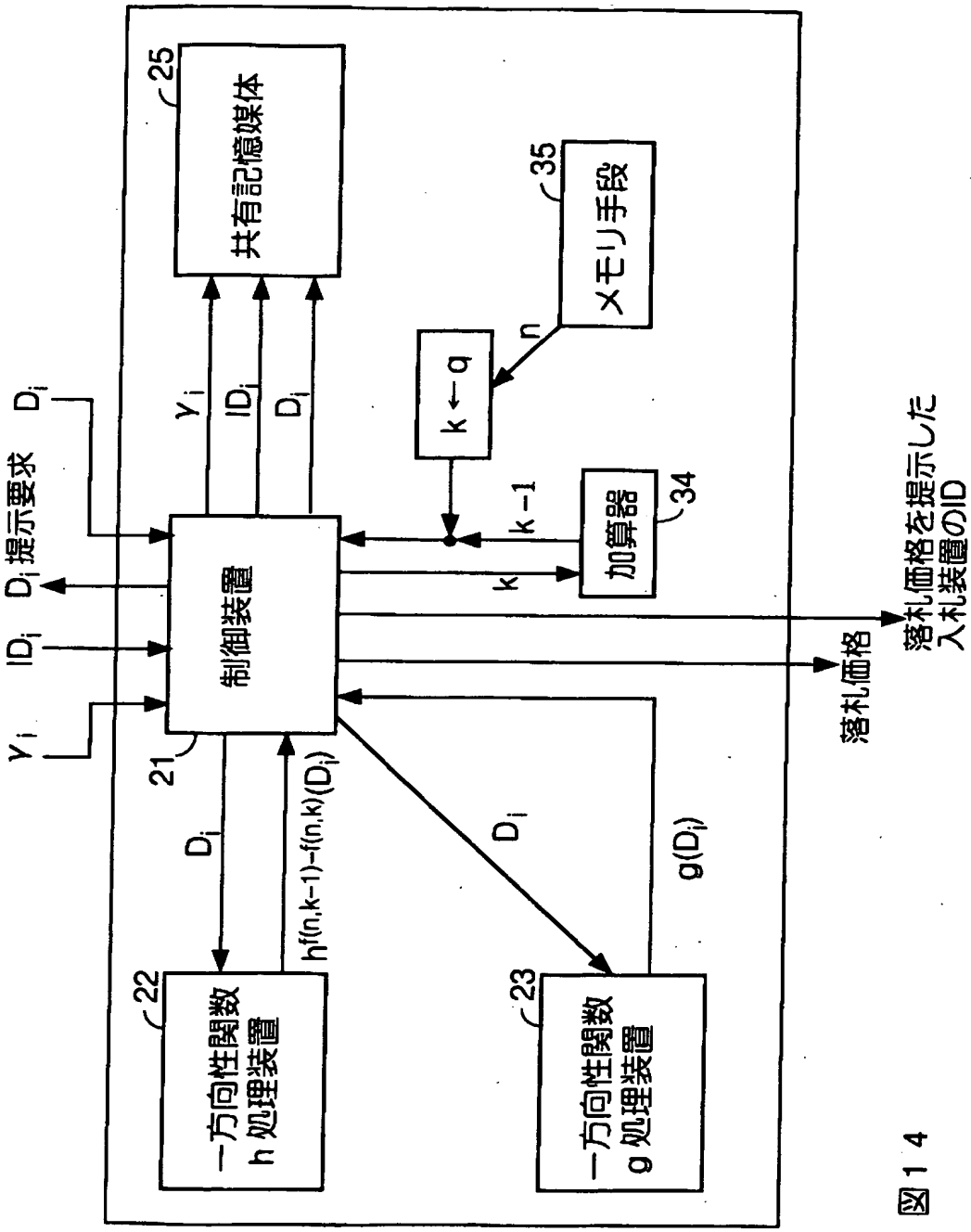
25
共有記憶媒体
35
メモリ手段
n
k←q
k
k−1
加算器
34
制御装置
21
D_i
ID_i
Y_i
D_i 提示要求
落札価格
落札価格を提示した入札装置のID
$h^{f(n,k-1)-f(n,k)}(D_i)$
$g(D_i)$
22
一方向性関数 h 処理装置
23
一方向性関数 g 処理装置

図１４

【図１５】

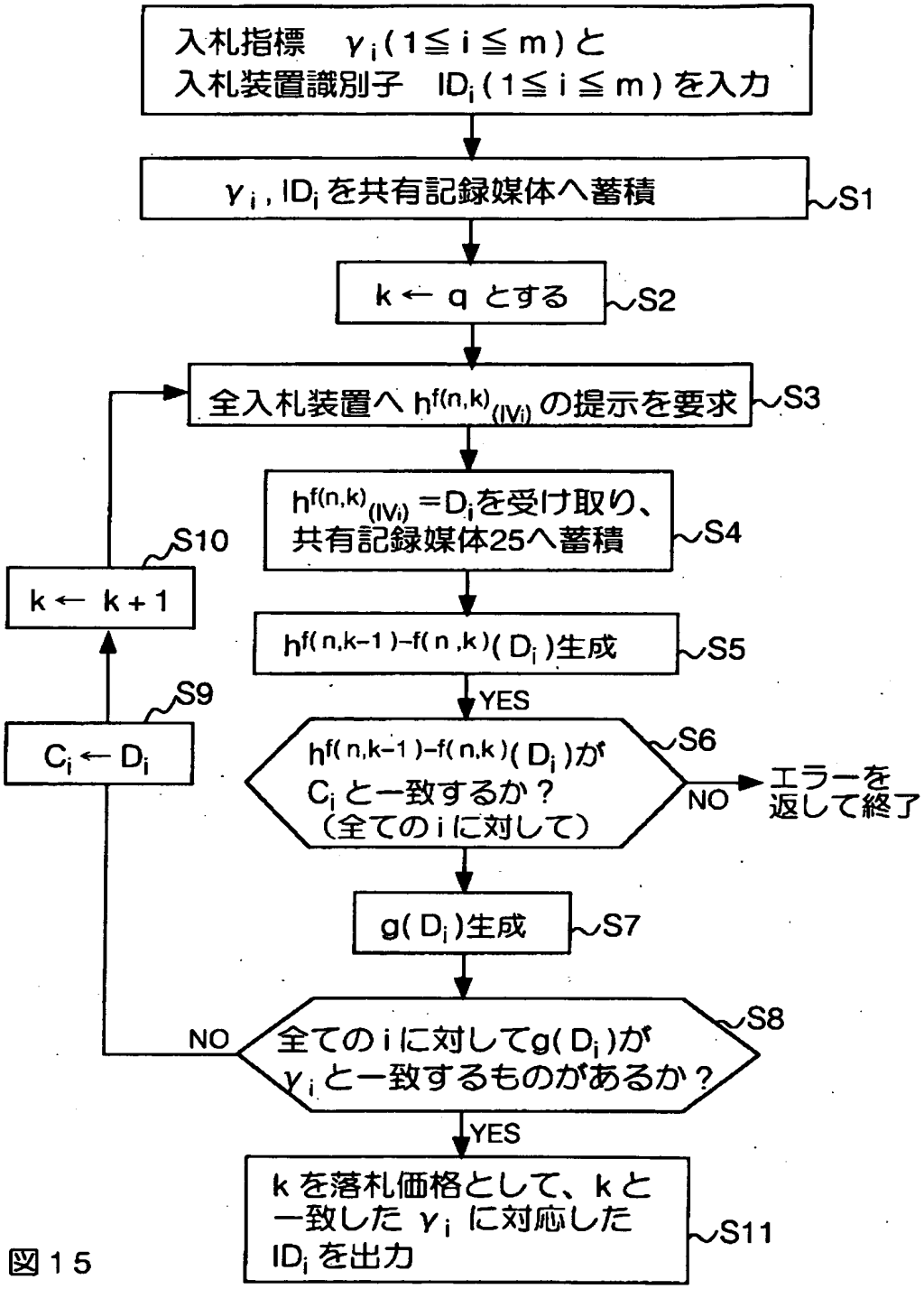
入札指標　γ_i（1≦i≦m）と
入札装置識別子　ID_i（1≦i≦m）を入力
γ_i，ID_iを共有記録媒体へ蓄積
S1
k ← q とする
S2
全入札装置へ $h^{f(n,k)}_{(IVi)}$ の提示を要求
S3
$h^{f(n,k)}_{(IVi)}$ ＝D_iを受け取り、
共有記録媒体25へ蓄積
S4
$h^{f(n,k-1)-f(n,k)}(D_i)$生成
S5
YES
$h^{f(n,k-1)-f(n,k)}(D_i)$が
C_iと一致するか？
（全てのiに対して）
S6
NO
エラーを
返して終了
g(D_i)生成
S7
全てのiに対してg(D_i)が
γ_iと一致するものがあるか？
S8
NO
YES
kを落札価格として、kと
一致した γ_i に対応した
ID_iを出力
S11
k ← k＋1
S10
C_i ← D_i
S9

図１５

【図１６】

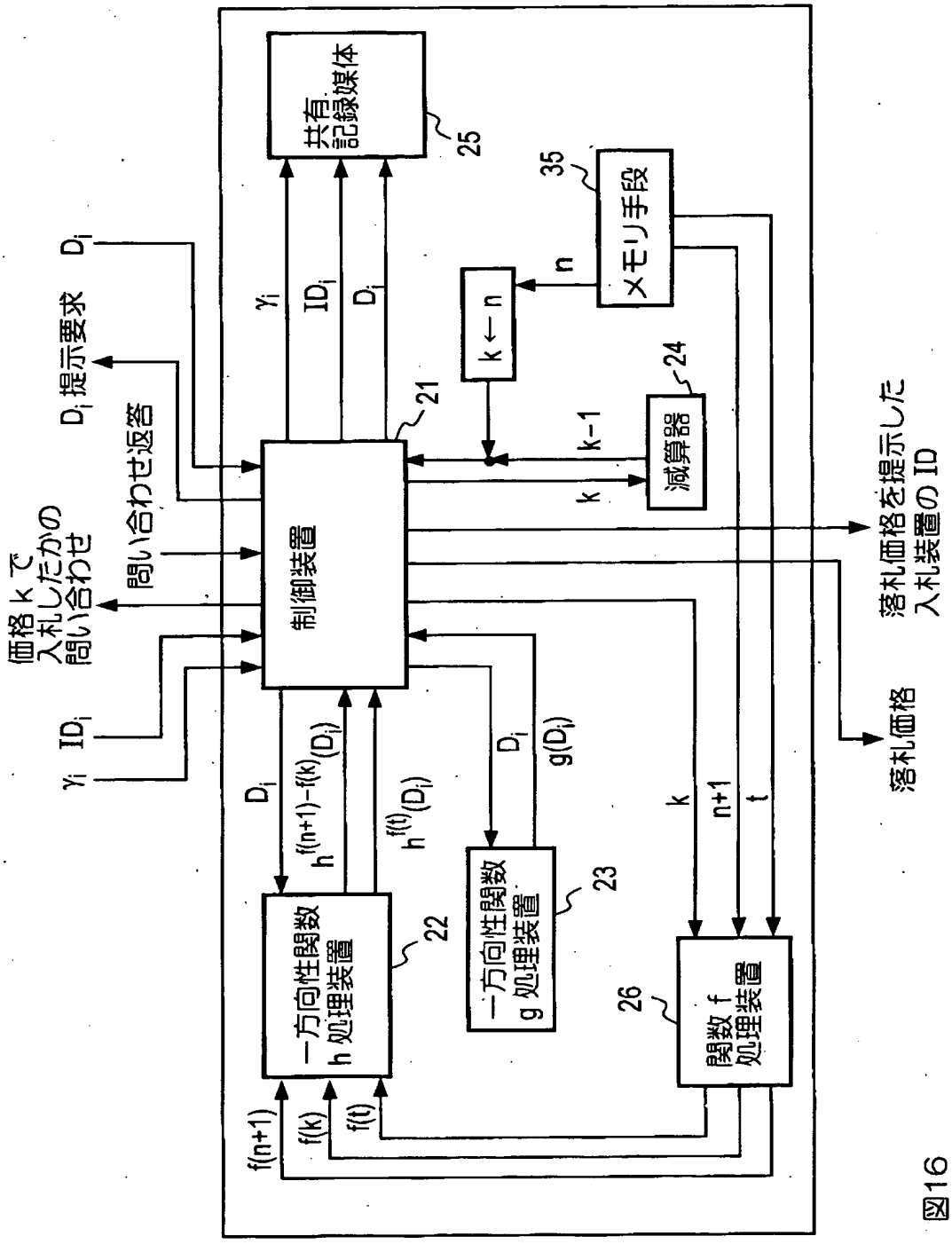
共有記録媒体
25
35
メモリ手段
n
k←n
24
減算器
k-1
k
21
制御装置
γ_i
ID_i
D_i
D_i 提示要求
問い合わせ返答
価格ｋで入札したかの問い合わせ
落札価格を提示した入札装置のID
落札価格
$h^{f(n+1)-f(k)}(D_i)$
$h^{f(t)}(D_i)$
$g(D_i)$
k
n+1
t
一方向性関数 h 処理装置
22
一方向性関数 g 処理装置
23
関数 f 処理装置
26
f(n+1)
f(k)
f(t)

図16

【図１７】

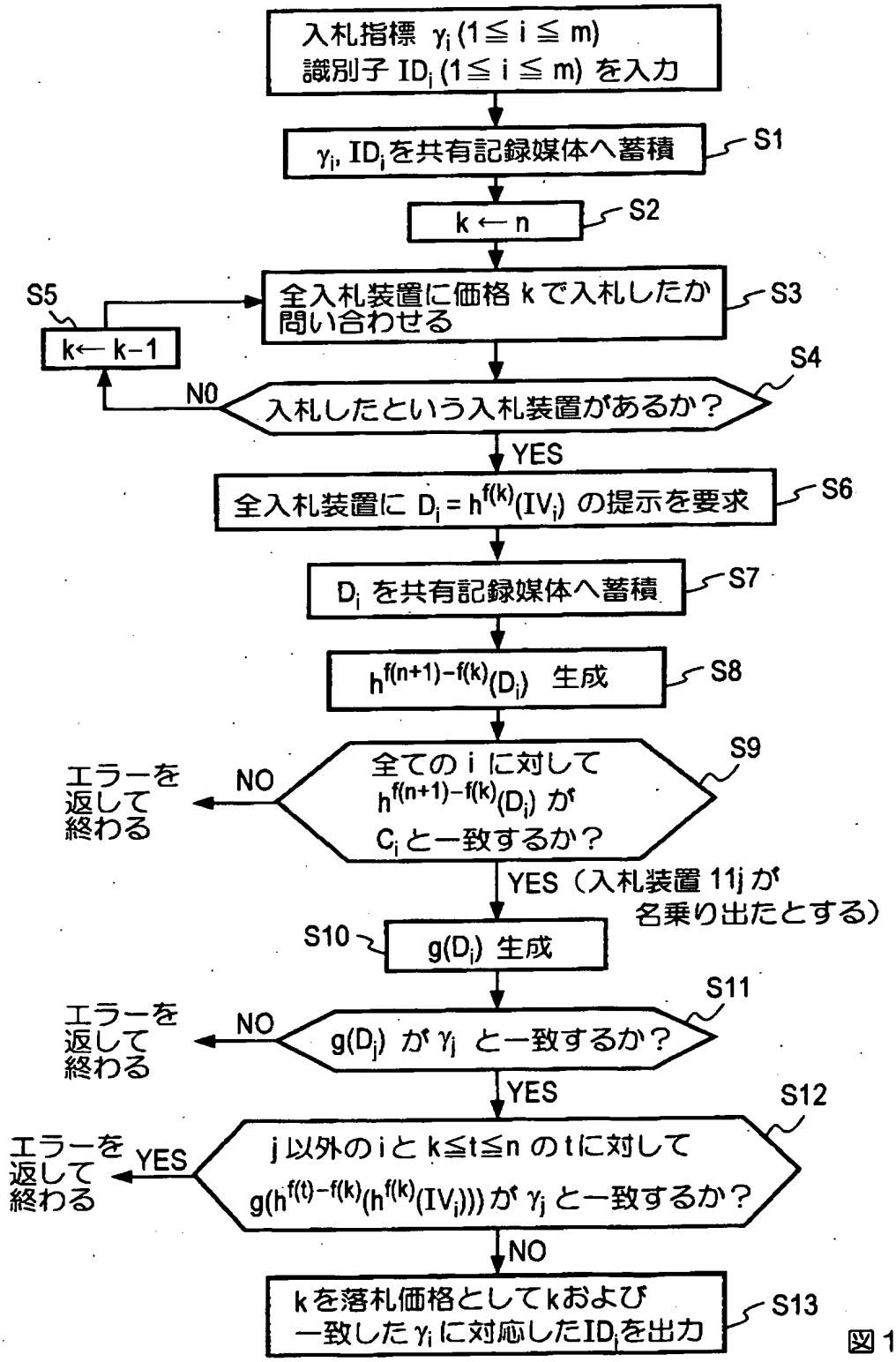
入札指標 γ_i (1≦i≦m)
識別子 ID_i (1≦i≦m) を入力
γ_i, ID_i を共有記録媒体へ蓄積
S1
k ← n
S2
全入札装置に価格 k で入札したか問い合わせる
S3
S5
k← k−1
S4
N0
入札したという入札装置があるか？
YES
全入札装置に $D_i = h^{f(k)}(IV_i)$ の提示を要求
S6
D_i を共有記録媒体へ蓄積
S7
$h^{f(n+1)-f(k)}(D_i)$ 生成
S8
全てのiに対して $h^{f(n+1)-f(k)}(D_i)$ が C_i と一致するか？
S9
NO
エラーを返して終わる
YES（入札装置 11j が名乗り出たとする）
S10
$g(D_i)$ 生成
S11
$g(D_j)$ が γ_j と一致するか？
NO
エラーを返して終わる
YES
S12
j以外のiと k≦t≦n のtに対して $g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ が γ_j と一致するか？
YES
エラーを返して終わる
NO
kを落札価格としてkおよび一致した γ_i に対応した ID_i を出力
S13

図１７

【図１８】

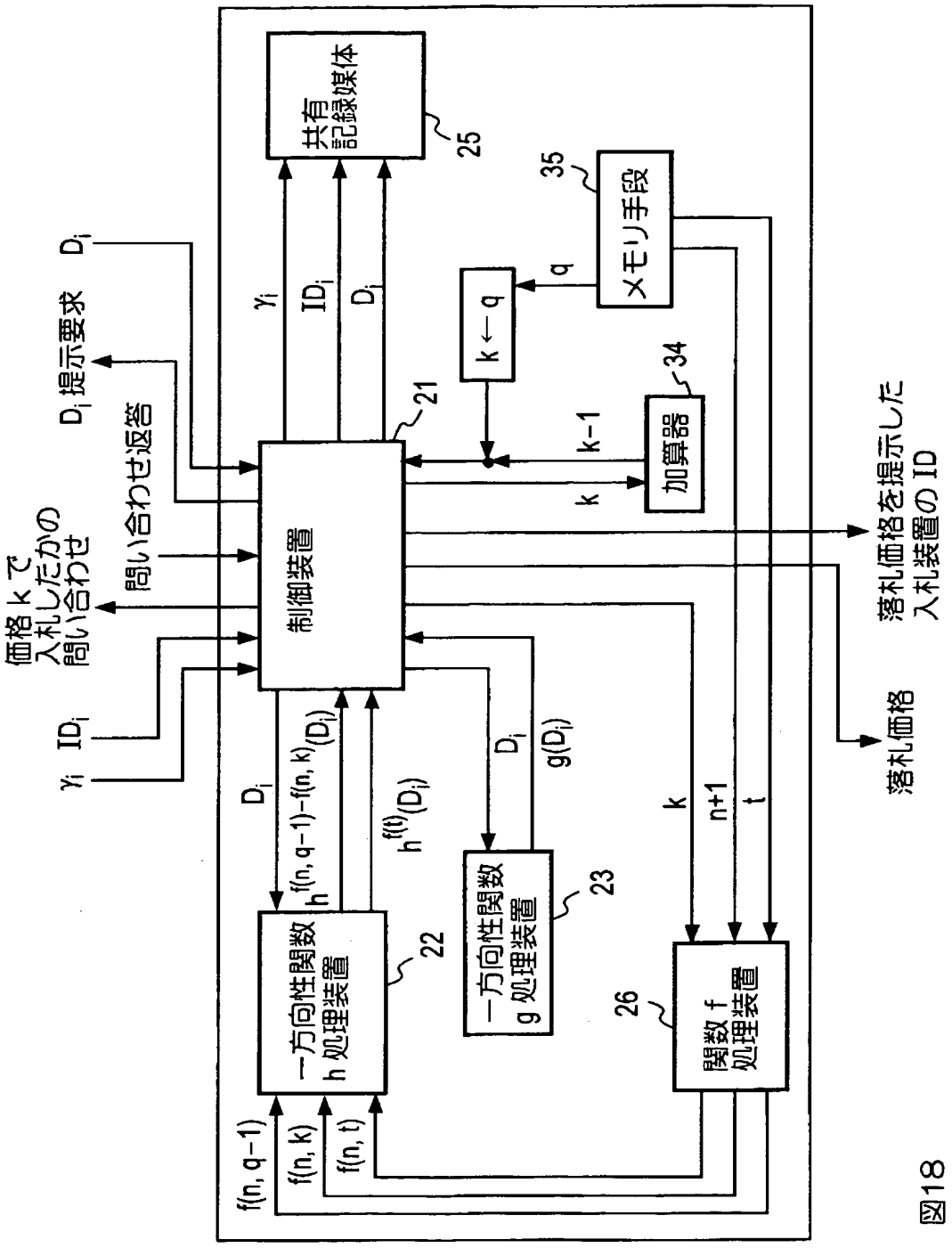
共有記録媒体
25
35
メモリ手段
q
k←q
34
加算器
k-1
k
21
制御装置
γi
IDi
Di
Di 提示要求
問い合わせ返答
価格ｋで入札したかの問い合わせ
落札価格を提示した入札装置のID
落札価格
一方向性関数 h 処理装置
22
一方向性関数 g 処理装置
23
関数 f 処理装置
26
h^(f(n,q-1)-f(n,k))(Di)
h^(f(t))(Di)
g(Di)
k
n+1
t
f(n,q-1)
f(n,k)
f(n,t)

図18

【図１９】

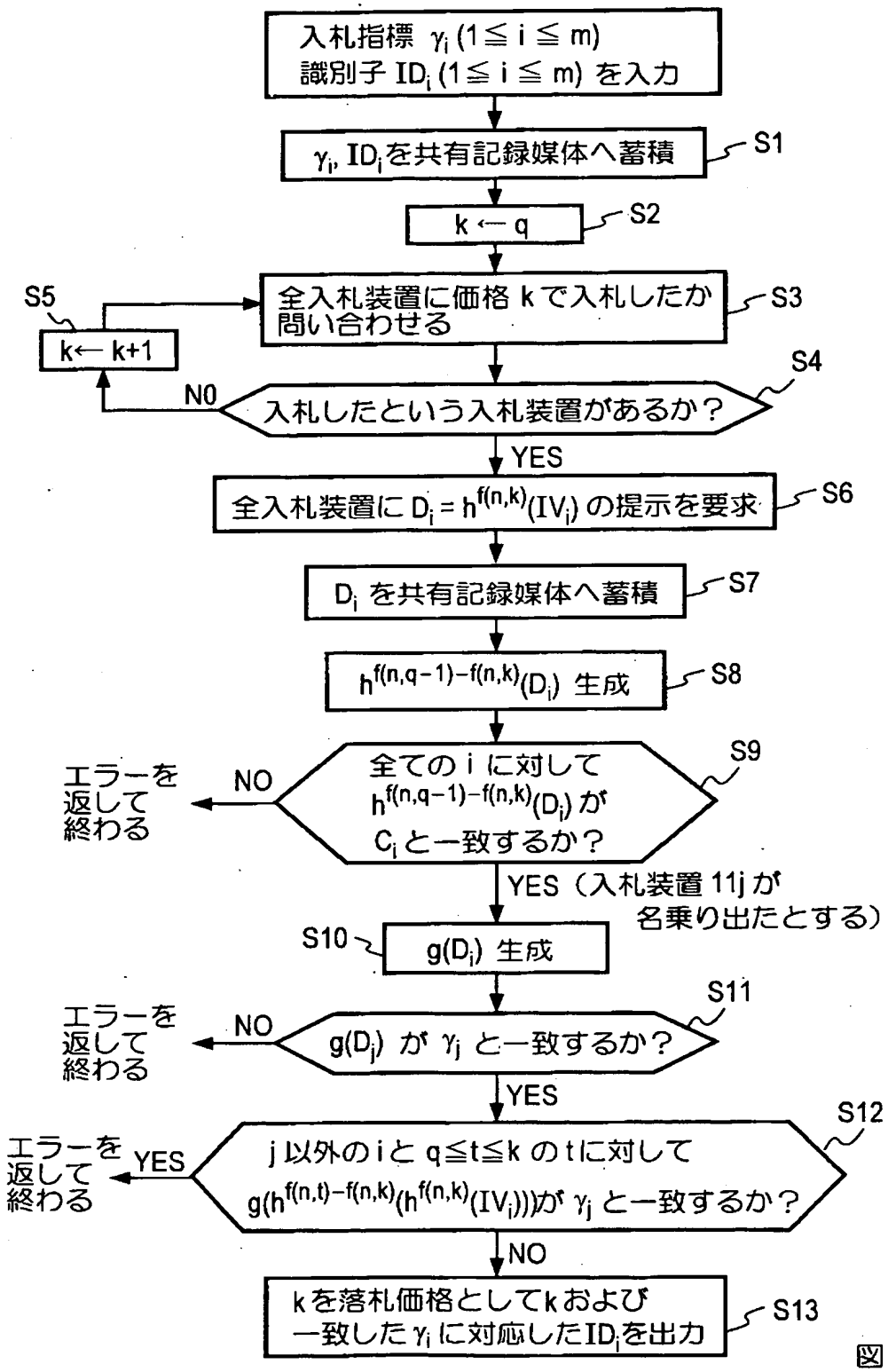
入札指標 γ_i (1≦i≦m)
識別子 ID_i (1≦i≦m) を入力
γ_i, ID_iを共有記録媒体へ蓄積
S1
k ← q
S2
全入札装置に価格 k で入札したか問い合わせる
S3
S5
k← k+1
S4
N0
入札したという入札装置があるか？
YES
全入札装置に $D_i = h^{f(n,k)}(IV_i)$ の提示を要求
S6
D_i を共有記録媒体へ蓄積
S7
$h^{f(n,q-1)-f(n,k)}(D_i)$ 生成
S8
全てのiに対して $h^{f(n,q-1)-f(n,k)}(D_i)$ が C_i と一致するか？
S9
エラーを返して終わる
NO
YES（入札装置 11j が名乗り出たとする）
S10
$g(D_i)$ 生成
S11
エラーを返して終わる
NO
$g(D_j)$ が γ_j と一致するか？
YES
S12
エラーを返して終わる
YES
j以外のiと q≦t≦k のtに対して $g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$が γ_j と一致するか？
NO
kを落札価格としてkおよび一致したγ_iに対応したID_iを出力
S13

図１９

【図２０】

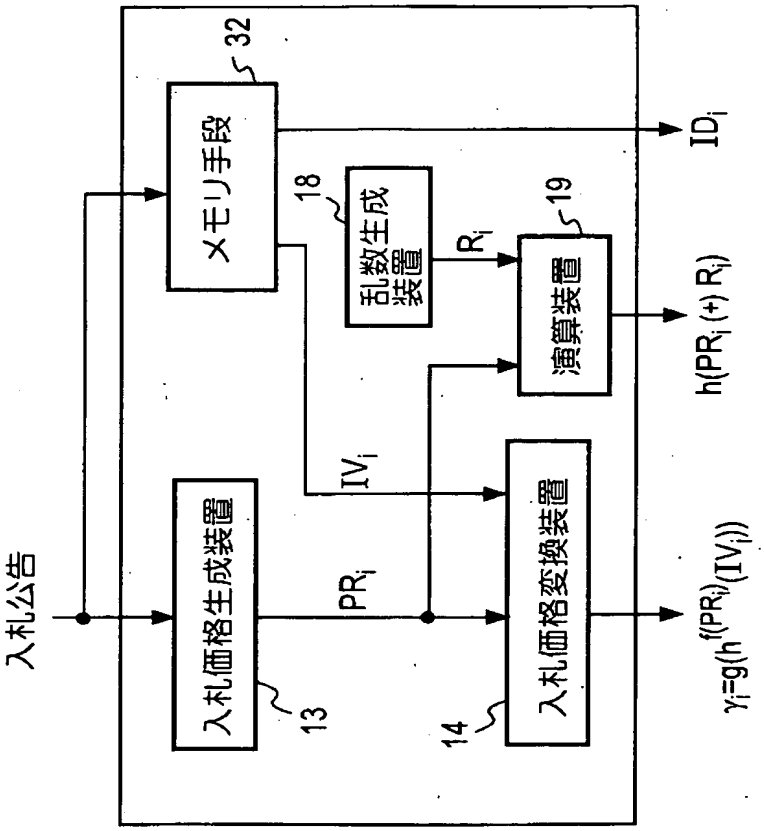
入札公告
入札価格生成装置
13
メモリ手段
32
乱数生成装置
18
演算装置
19
入札価格変換装置
14
PRi
IVi
Ri
IDi
h(PRi (+) Ri)
γi=g(h^f(PRi)(IVi))

図20

【図２１】

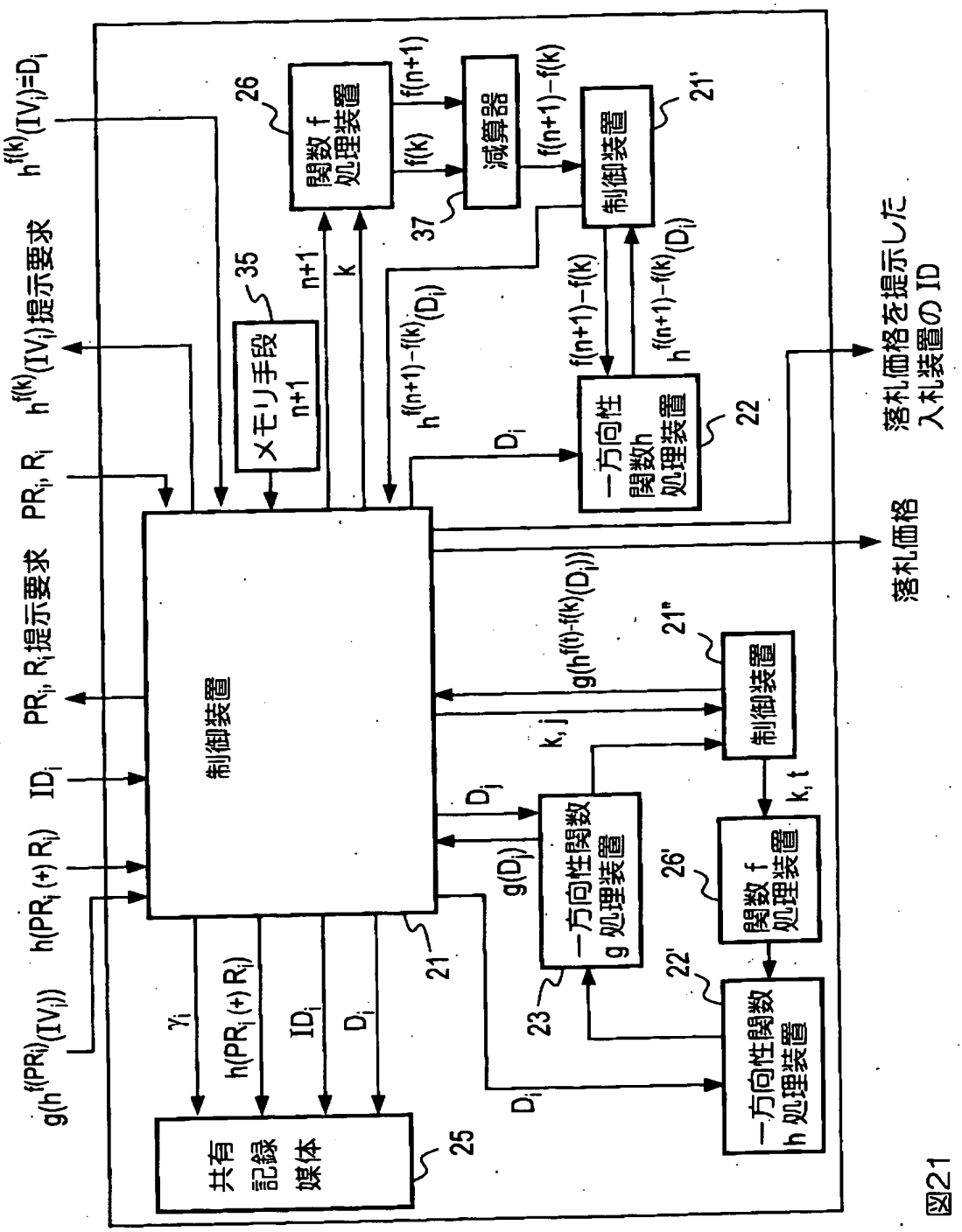
制御装置
共有記録媒体
25
一方向性関数g処理装置
23
一方向性関数h処理装置
22
22'
関数f処理装置
26
26'
減算器
37
メモリ手段
n+1
35
制御装置
21
21'
21"
一方向性関数h処理装置
22
落札価格
落札価格を提示した入札装置のID
$h^{f(k)}(IV_i)=D_i$
$h^{f(k)}(IV_i)$提示要求
PR_i, R_i
PR_i, R_i提示要求
ID_i
$h(PR_i(+)R_i)$
$g(h^{f(PR_i)}(IV_i))$
γ_i
D_i
$g(D_i)$
k, j
k, t
n+1
k
f(n+1)
f(k)
f(n+1)−f(k)
$h^{f(n+1)-f(k)}(D_i)$
$g(h^{f(i)-f(k)}(D_i))$

図21

【図２２】

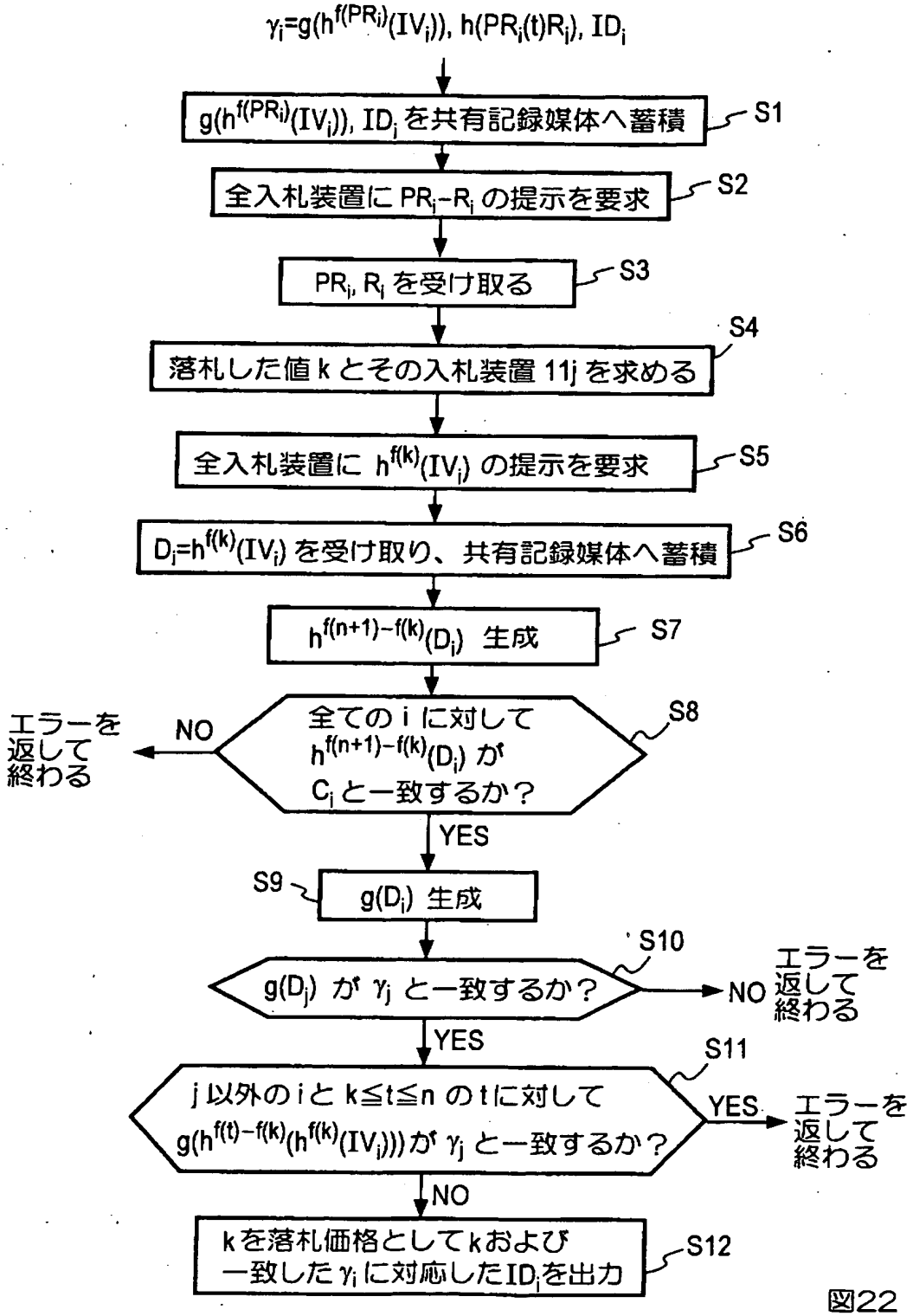
$\gamma_i=g(h^{f(PR_i)}(IV_i)), h(PR_i(t)R_i), ID_i$
$g(h^{f(PR_i)}(IV_i)), ID_i$ を共有記録媒体へ蓄積
S1
全入札装置に PR_i-R_i の提示を要求
S2
PR_i, R_i を受け取る
S3
落札した値 k とその入札装置 11j を求める
S4
全入札装置に $h^{f(k)}(IV_i)$ の提示を要求
S5
$D_i=h^{f(k)}(IV_i)$ を受け取り、共有記録媒体へ蓄積
S6
$h^{f(n+1)-f(k)}(D_i)$ 生成
S7
全ての i に対して $h^{f(n+1)-f(k)}(D_i)$ が C_i と一致するか？
S8
NO
エラーを返して終わる
YES
S9
$g(D_i)$ 生成
S10
$g(D_j)$ が γ_j と一致するか？
NO
エラーを返して終わる
YES
S11
j 以外の i と $k \leqq t \leqq n$ の t に対して $g(h^{f(t)-f(k)}(h^{f(k)}(IV_i)))$ が γ_j と一致するか？
YES
エラーを返して終わる
NO
k を落札価格として k および一致した γ_i に対応した ID_i を出力
S12

図22

【図２３】

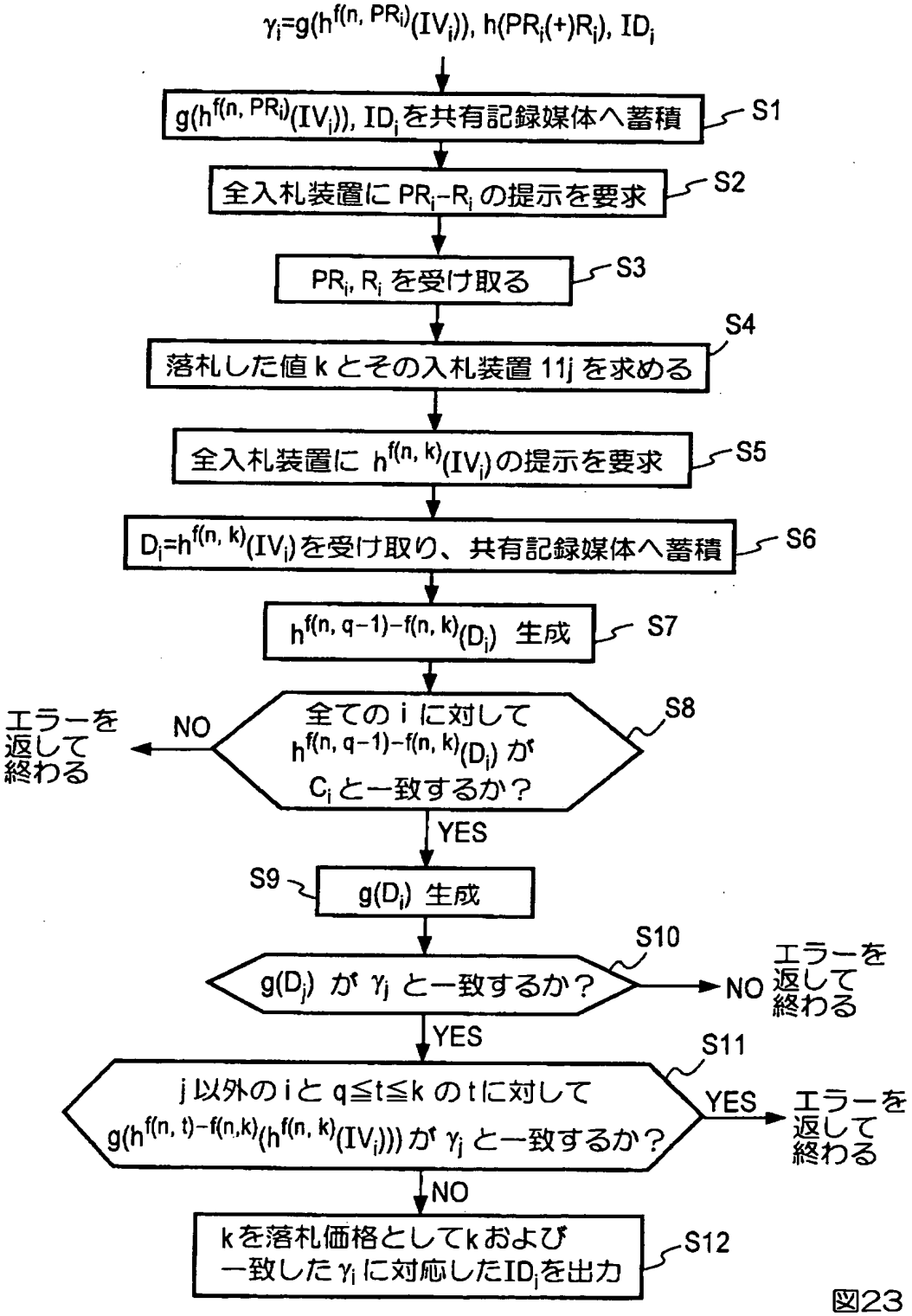
$\gamma_i=g(h^{f(n,PR_i)}(IV_i)), h(PR_i(+)R_i), ID_i$
$g(h^{f(n,PR_i)}(IV_i)), ID_i$を共有記録媒体へ蓄積
S1
全入札装置にPR_i-R_iの提示を要求
S2
PR_i, R_iを受け取る
S3
落札した値kとその入札装置11jを求める
S4
全入札装置に$h^{f(n,k)}(IV_i)$の提示を要求
S5
$D_i=h^{f(n,k)}(IV_i)$を受け取り、共有記録媒体へ蓄積
S6
$h^{f(n,q-1)-f(n,k)}(D_i)$ 生成
S7
全てのiに対して$h^{f(n,q-1)-f(n,k)}(D_i)$がC_iと一致するか？
S8
NO
エラーを返して終わる
YES
S9
$g(D_i)$ 生成
$g(D_j)$がγ_jと一致するか？
S10
NO
エラーを返して終わる
YES
j以外のiとq≦t≦kのtに対して$g(h^{f(n,t)-f(n,k)}(h^{f(n,k)}(IV_i)))$が$\gamma_j$と一致するか？
S11
YES
エラーを返して終わる
NO
kを落札価格としてkおよび一致したγ_iに対応したID_iを出力
S12

図23

【図２４】

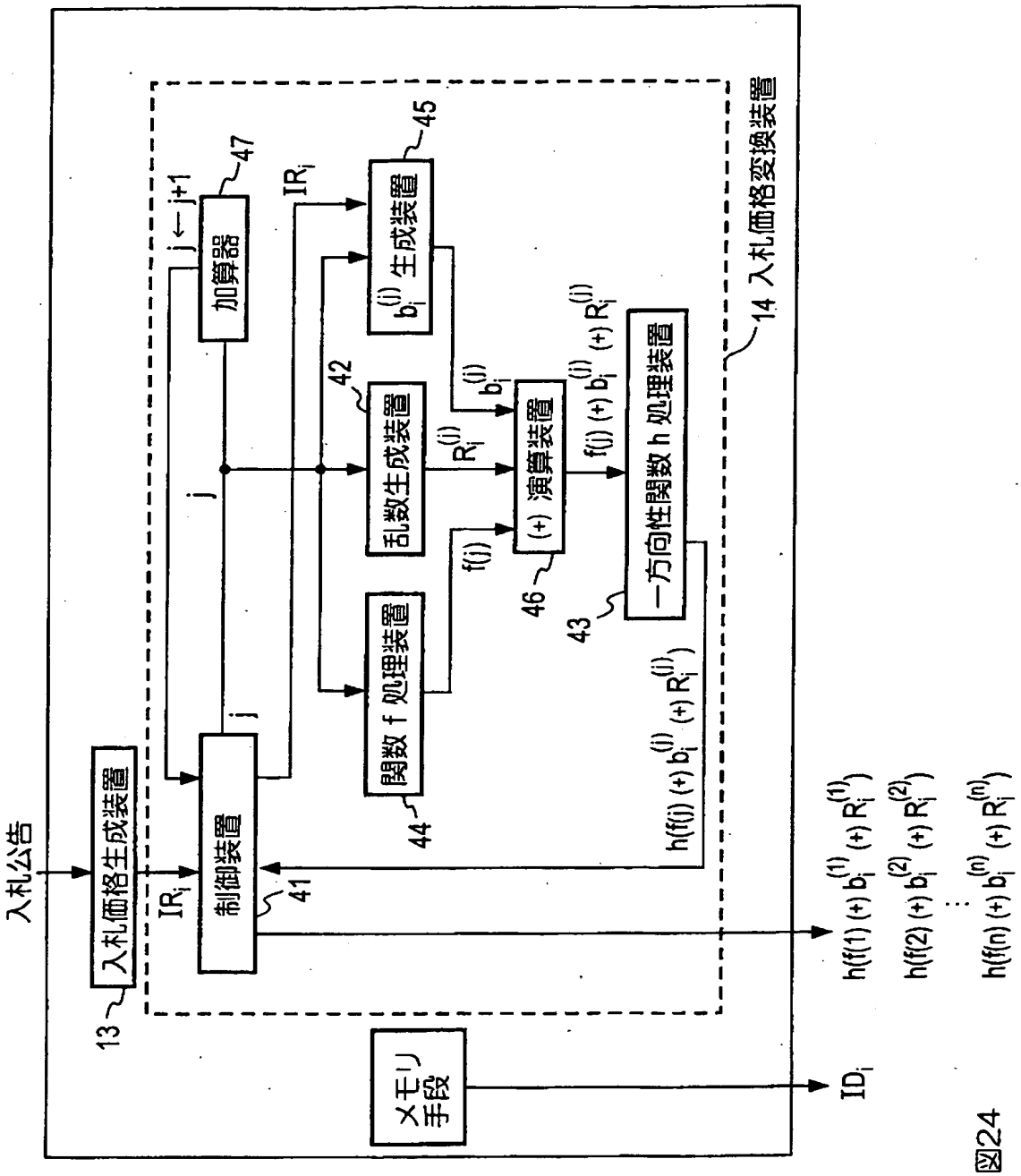
入札公告
入札価格生成装置
13
制御装置
41
IRi
j
j ← j+1
加算器
47
IRi
乱数生成装置
42
関数 f 処理装置
44
f(j)
(+) 演算装置
46
f(j) (+) bi(j) (+) Ri(j)
一方向性関数 h 処理装置
43
h(f(j) (+) bi(j) (+) Ri(j))
bi(j) 生成装置
45
bi(j)
Ri(j)
14 入札価格変換装置
メモリ手段
IDi
h(f(1) (+) bi(1) (+) Ri(1))
h(f(2) (+) bi(2) (+) Ri(2))
h(f(n) (+) bi(n) (+) Ri(n))

図24

【図２５】

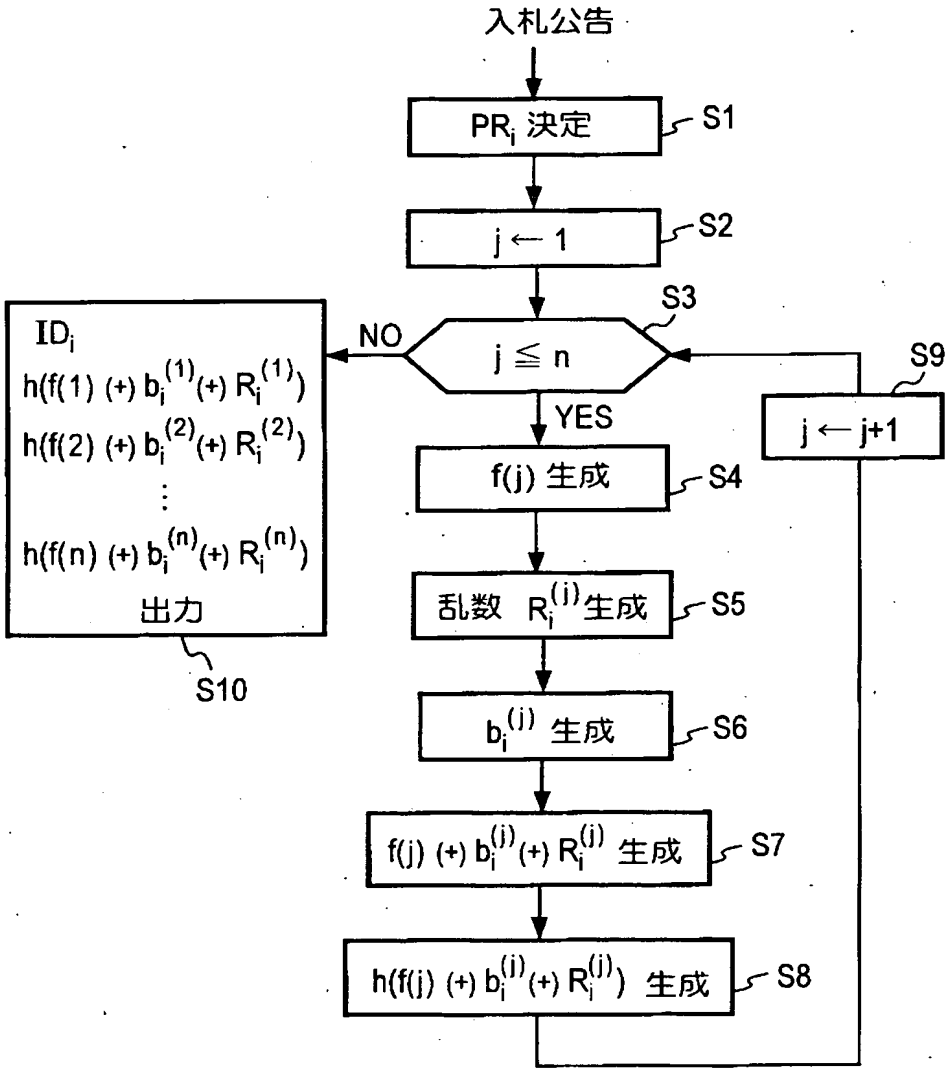
入札公告
PR$_i$ 決定
S1
j ← 1
S2
S3
j ≦ n
NO
YES
S9
j ← j+1
f(j) 生成
S4
乱数 R$_i^{(j)}$生成
S5
b$_i^{(j)}$ 生成
S6
f(j) (+) b$_i^{(j)}$(+) R$_i^{(j)}$ 生成
S7
h(f(j) (+) b$_i^{(j)}$(+) R$_i^{(j)}$) 生成
S8
ID$_i$
h(f(1) (+) b$_i^{(1)}$(+) R$_i^{(1)}$)
h(f(2) (+) b$_i^{(2)}$(+) R$_i^{(2)}$)
⋮
h(f(n) (+) b$_i^{(n)}$(+) R$_i^{(n)}$)
出力
S10

図25

【図２６】

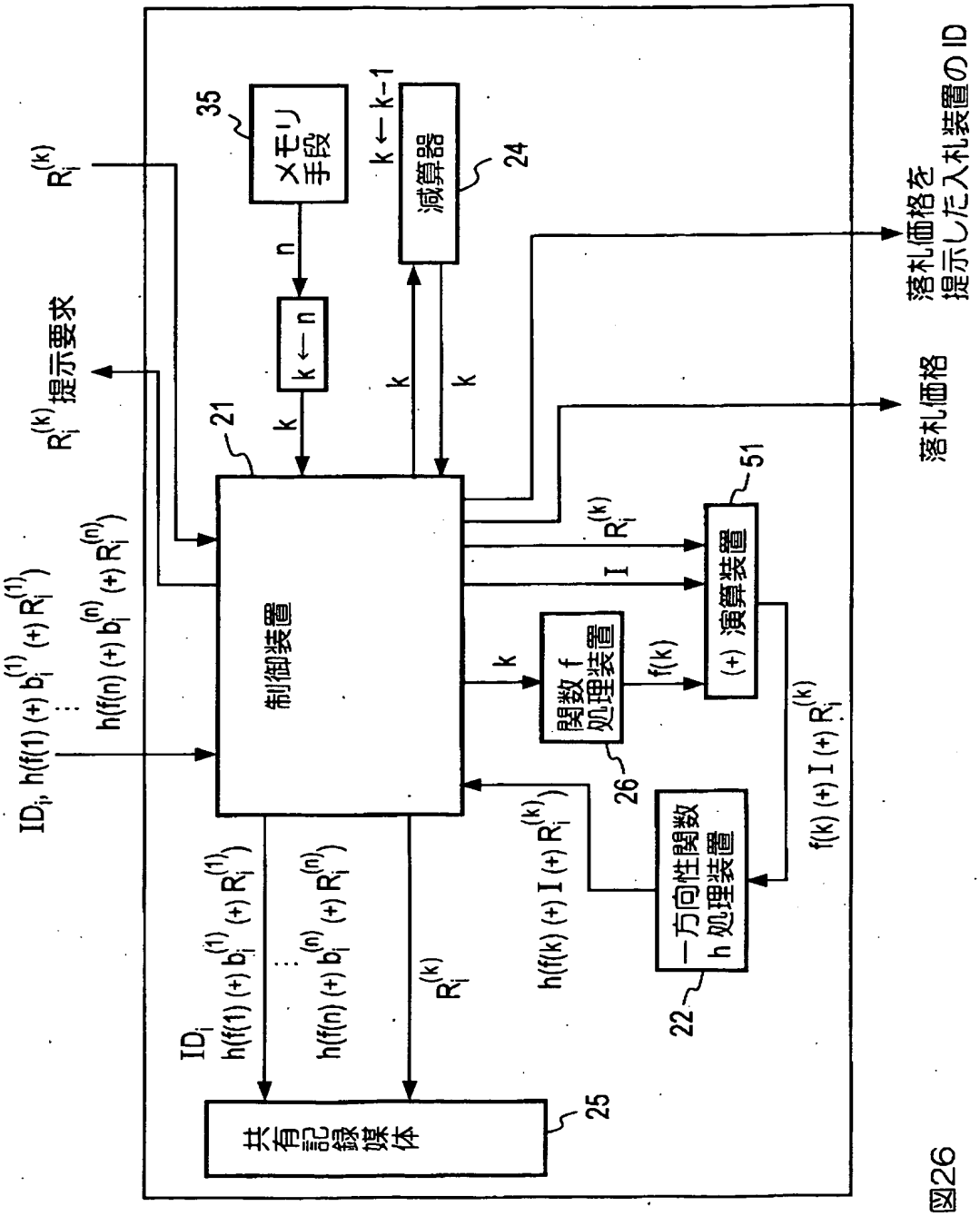
制御装置
21
メモリ手段
35
減算器
24
k←k-1
k←n
n
k
$R_i^{(k)}$
$R_i^{(k)}$提示要求
落札価格を
提示した入札装置のID
落札価格
$ID_i, h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}) \cdots h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})$
I
関数 f 処理装置
f(k)
26
(+) 演算装置
51
$f(k)(+)I(+)R_i^{(k)}$
一方向性関数 h 処理装置
22
$h(f(k)(+)I(+)R_i^{(k)})$
ID_i
$h(f(1)(+)b_i^{(1)}(+)R_i^{(1)}) \cdots h(f(n)(+)b_i^{(n)}(+)R_i^{(n)})$
$R_i^{(k)}$
共有記録媒体
25

図26

【図２７】

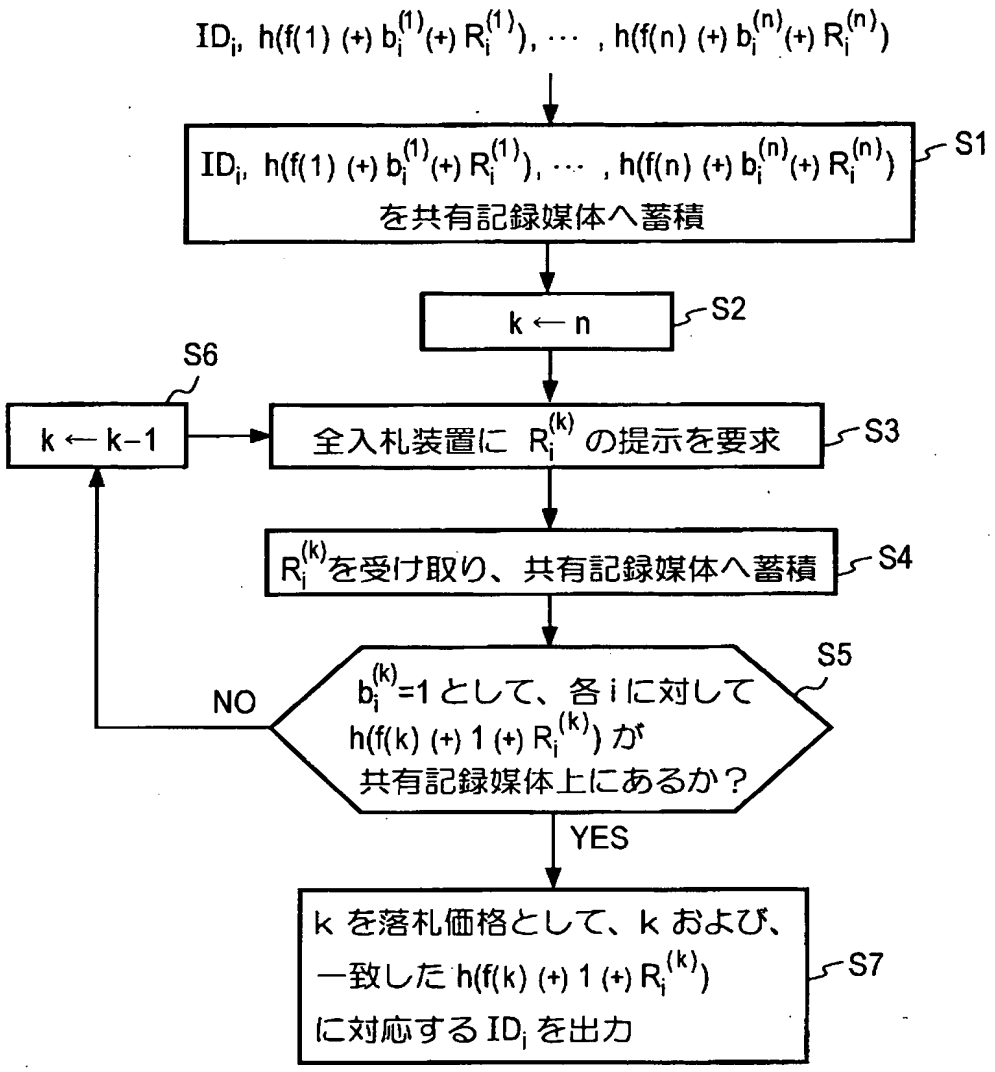
ID_i, $h(f(1) (+) b_i^{(1)} (+) R_i^{(1)}), \cdots, h(f(n) (+) b_i^{(n)} (+) R_i^{(n)})$
ID_i, $h(f(1) (+) b_i^{(1)} (+) R_i^{(1)}), \cdots, h(f(n) (+) b_i^{(n)} (+) R_i^{(n)})$
を共有記録媒体へ蓄積
S1
k ← n
S2
S6
k ← k−1
全入札装置に $R_i^{(k)}$ の提示を要求
S3
$R_i^{(k)}$を受け取り、共有記録媒体へ蓄積
S4
$b_i^{(k)}$=1 として、各 i に対して
$h(f(k) (+) 1 (+) R_i^{(k)})$ が
共有記録媒体上にあるか？
S5
NO
YES
k を落札価格として、k および、
一致した $h(f(k) (+) 1 (+) R_i^{(k)})$
に対応する ID_i を出力
S7

図27

【図２８】

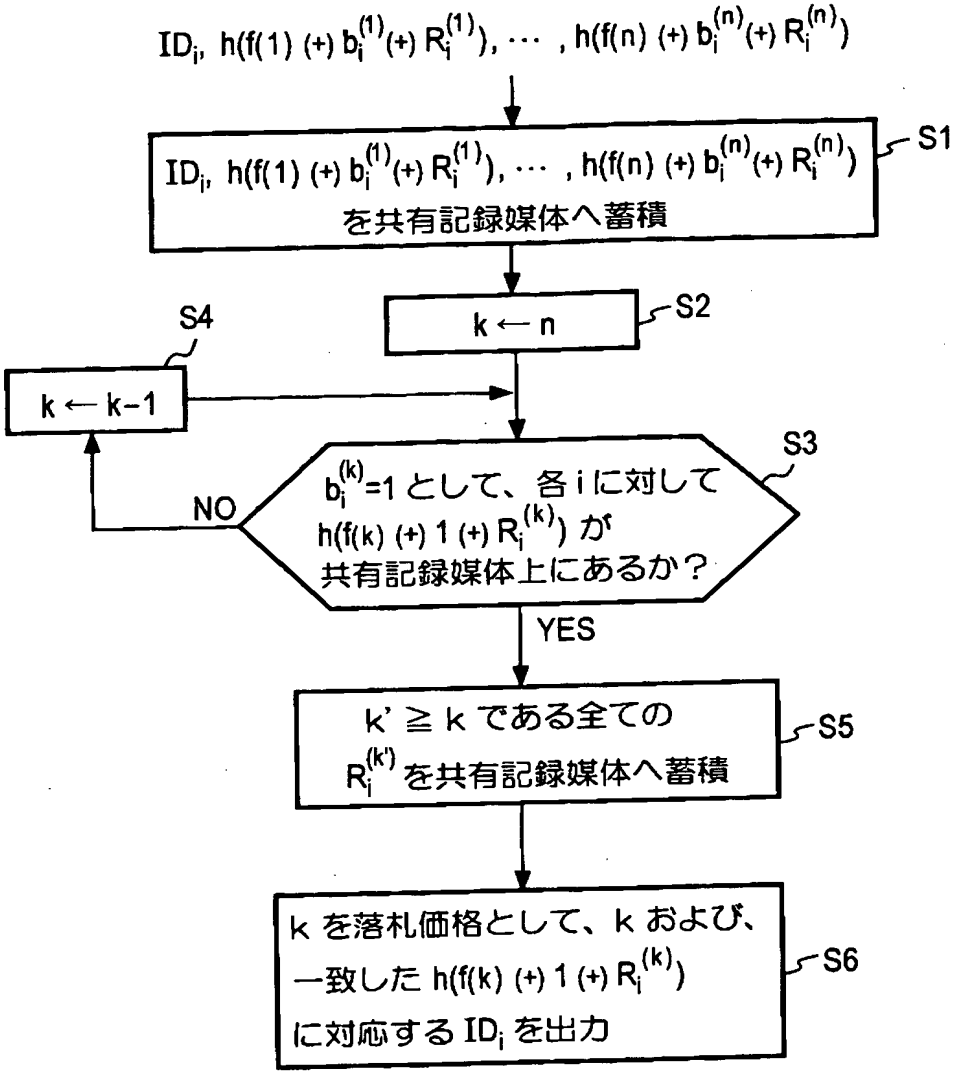
ID_i, $h(f(1)\ (+)\ b_i^{(1)}\ (+)\ R_i^{(1)}), \cdots, h(f(n)\ (+)\ b_i^{(n)}\ (+)\ R_i^{(n)})$
ID_i, $h(f(1)\ (+)\ b_i^{(1)}\ (+)\ R_i^{(1)}), \cdots, h(f(n)\ (+)\ b_i^{(n)}\ (+)\ R_i^{(n)})$
を共有記録媒体へ蓄積
S1
$k \leftarrow n$
S2
S4
$k \leftarrow k-1$
$b_i^{(k)}=1$ として、各 i に対して
$h(f(k)\ (+)\ 1\ (+)\ R_i^{(k)})$ が
共有記録媒体上にあるか？
S3
NO
YES
$k' \geqq k$ である全ての
$R_i^{(k')}$ を共有記録媒体へ蓄積
S5
k を落札価格として、k および、
一致した $h(f(k)\ (+)\ 1\ (+)\ R_i^{(k)})$
に対応する ID_i を出力
S6

図28

【図２９】

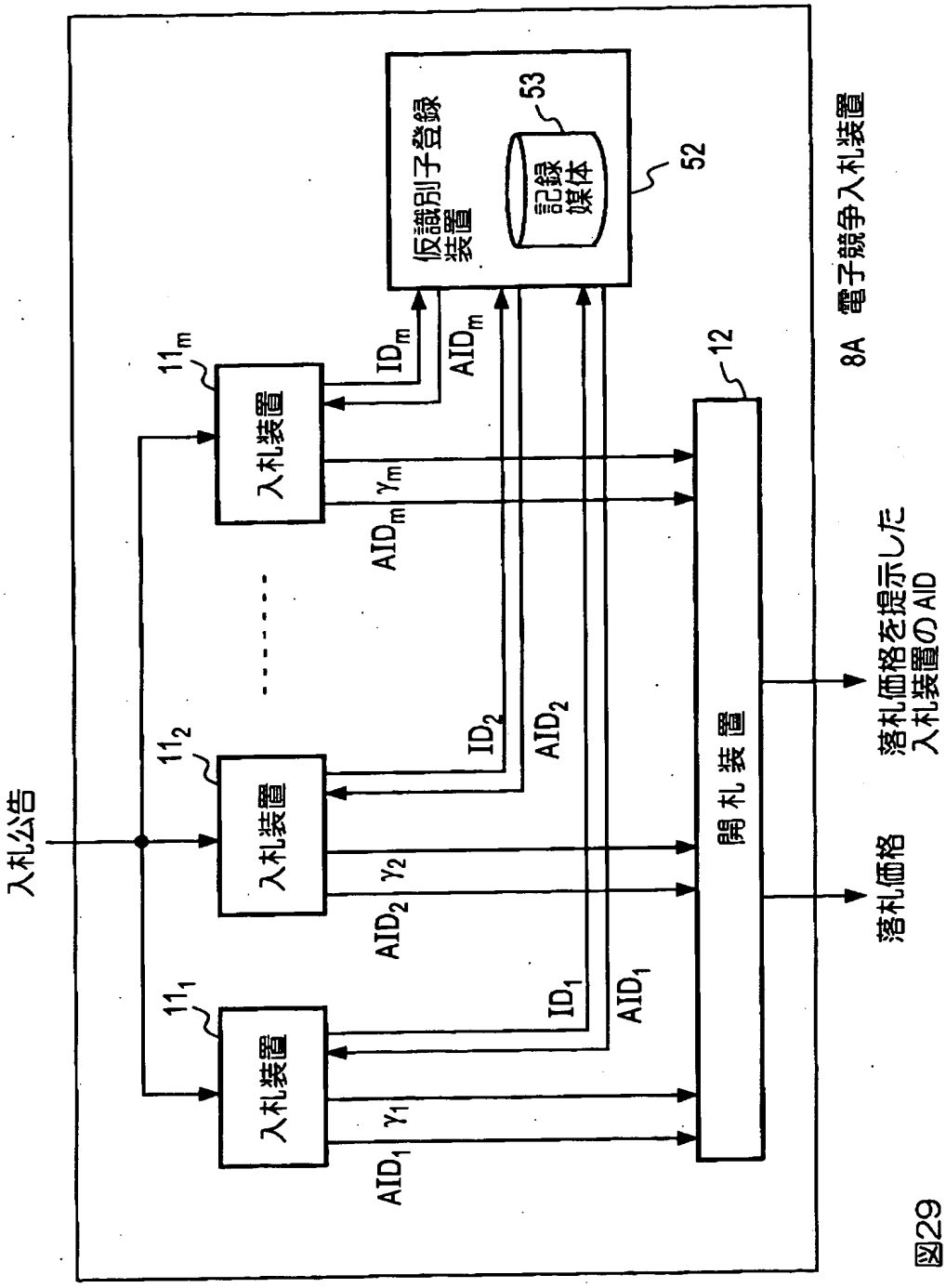
8A 電子競争入札装置
仮識別子登録装置
53
記録媒体
52
12
入札装置
11_m
11_2
11_1
ID_m
AID_m
γ_m
ID_2
AID_2
γ_2
ID_1
AID_1
γ_1
開札装置
入札公告
落札価格を提示した入札装置のAID
落札価格

図29

【図３０】

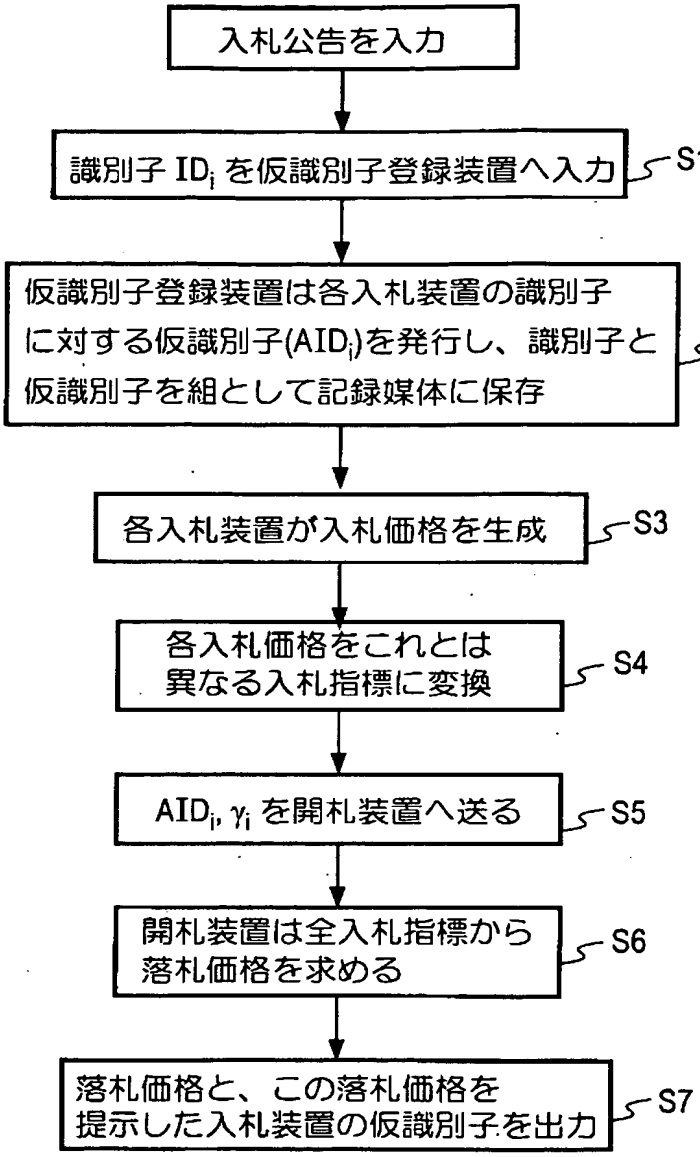
入札公告を入力
識別子 ID_i を仮識別子登録装置へ入力
S1
仮識別子登録装置は各入札装置の識別子に対する仮識別子(AID_i)を発行し、識別子と仮識別子を組として記録媒体に保存
S2
各入札装置が入札価格を生成
S3
各入札価格をこれとは異なる入札指標に変換
S4
AID_i, γ_i を開札装置へ送る
S5
開札装置は全入札指標から落札価格を求める
S6
落札価格と、この落札価格を提示した入札装置の仮識別子を出力
S7

図30

【書類名】　　要約書

【要約】

【課題】　入札価格PR_iが他の入札装置から知られない。

【解決手段】　入札装置11_iから入札指標$\gamma_i = g(h^{f(PRi)}(IV_i))$（$IV_i$は初期値、$h^{f(PRi)}$はハッシュ関数ｈをｆ（$PR_i$）回処理、ｇハッシュ関数）と入札装置$11_i$の$ID_i$を入力し、共有の記録媒体２５に蓄積し（Ｓ１）、ｋを入札の上限値ｎとし（Ｓ２）、ｉ＝１とし（Ｓ４）、ｆ（ｋ）を生成し（Ｓ７）、IV_iを初期値として$\delta_i = h^{f(k)}(IV_i)$を生成し（Ｓ８）、$\delta_i$（$-g(\delta_i)$を作る）（Ｓ９）、この$\delta_i$と一致する$\gamma_i$が記録媒体２５にあるかを調べ（Ｓ１０）、なければ、ｉを＋１して、次々と、各入札装置について調べ、全入札装置の数ｍについて調べ終ると、ｋを－１して、同様にして$\delta_i = g(h^{f(k)}(IV_i))$と一致する$\gamma_i$があるかを調べ、一致した時のｋを最高落札値とし、ｋとそのγ_iのID_iを出力する。

【選択図】　　図８

【書類名】　手続補正書
【整理番号】　NTTH115596
【提出日】　平成11年 7月22日
【あて先】　特許庁長官殿
【事件の表示】
　【出願番号】　平成11年特許願第205004号
【補正をする者】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100066153
　【弁理士】
　【氏名又は名称】　草野　　卓
　【電話番号】　03-3350-6456
【手続補正　1】
　【補正対象書類名】　図面
　【補正対象項目名】　図７
　【補正方法】　変更
　【補正の内容】　1
【手続補正　2】
　【補正対象書類名】　図面
　【補正対象項目名】　図１０
　【補正方法】　変更
　【補正の内容】　2
【手続補正　3】
　【補正対象書類名】　図面
　【補正対象項目名】　図１２
　【補正方法】　変更
　【補正の内容】　3

【手続補正　4】

【補正対象書類名】　図面

【補正対象項目名】　図１４

【補正方法】　変更

【補正の内容】　4

【プルーフの要否】　要

【図７】

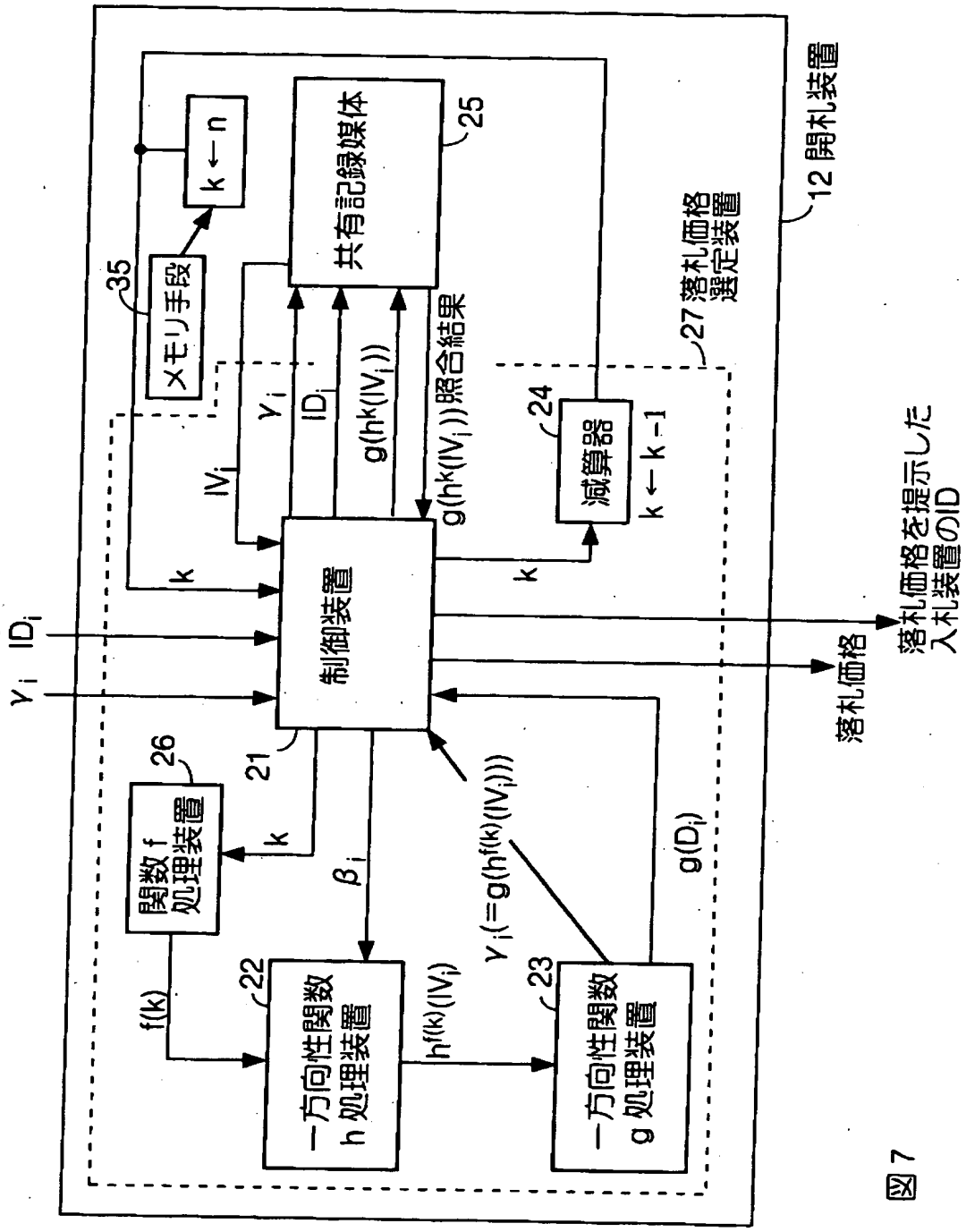
12 開札装置
共有記録媒体
25
k ← n
メモリ手段
35
27 落札価格選定装置
減算器
24
k ← k -1
制御装置
21
関数 f 処理装置
26
一方向性関数 h 処理装置
22
一方向性関数 g 処理装置
23
ID_i
γ_i
IV_i
k
β_i
f(k)
$h^{f(k)}(IV_i)$
$\gamma_i(=g(h^{f(k)}(IV_i)))$
$g(D_i)$
$g(h^k(IV_i))$照合結果
落札価格
落札価格を提示した入札装置のID

図７

【図１０】

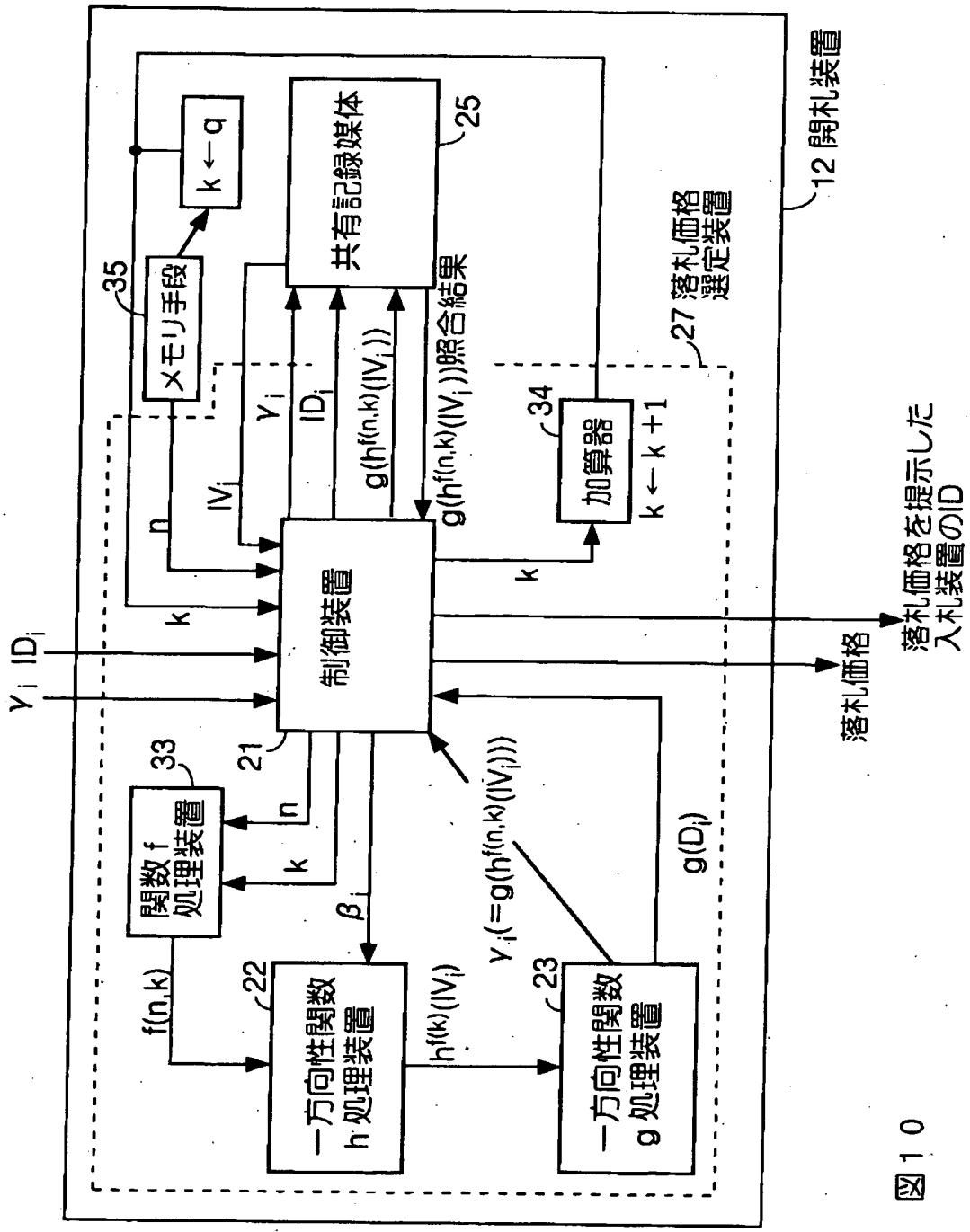
12 開札装置
27 落札価格選定装置
25
共有記録媒体
35
メモリ手段
k ← q
34
加算器
k ← k + 1
制御装置
21
33
関数 f 処理装置
22
一方向性関数 h 処理装置
23
一方向性関数 g 処理装置
落札価格
落札価格を提示した入札装置のID
g(h^f(n,k)(IVi))照合結果
IVi
IDi
γi
n
k
βi
f(n,k)
h^f(k)(IVi)
γi(=g(h^f(n,k)(IVi)))
g(Di)

図１０

【図１２】

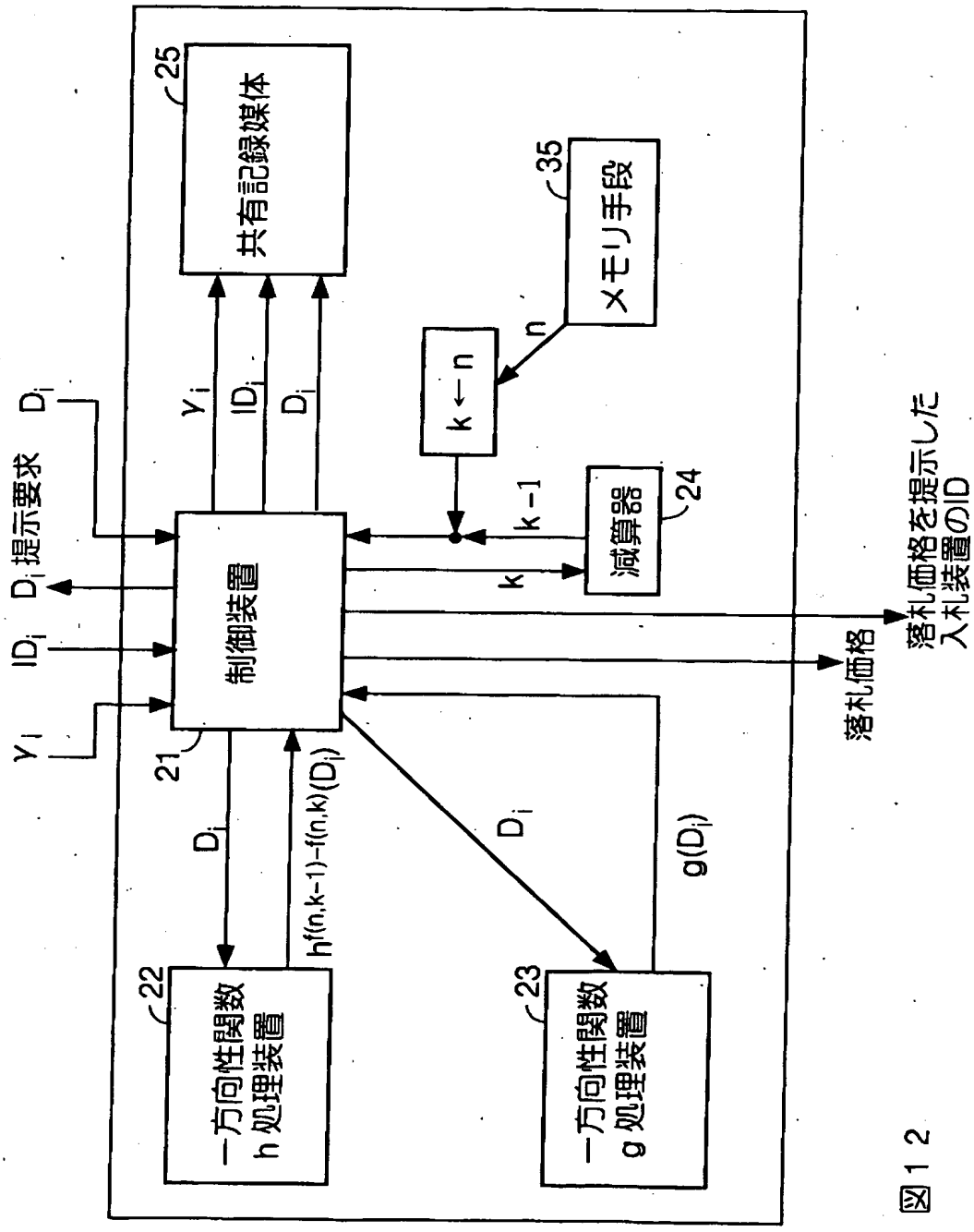
25
共有記録媒体
35
メモリ手段
n
k←n
Y_i
ID_i
D_i
D_i
D_i 提示要求
ID_i
Y_i
制御装置
21
k
k-1
減算器
24
落札価格を提示した入札装置のID
落札価格
D_i
$h^{f(n,k-1)-f(n,k)}(D_i)$
D_i
$g(D_i)$
22
一方向性関数 h 処理装置
23
一方向性関数 g 処理装置

図１２

【図１４】

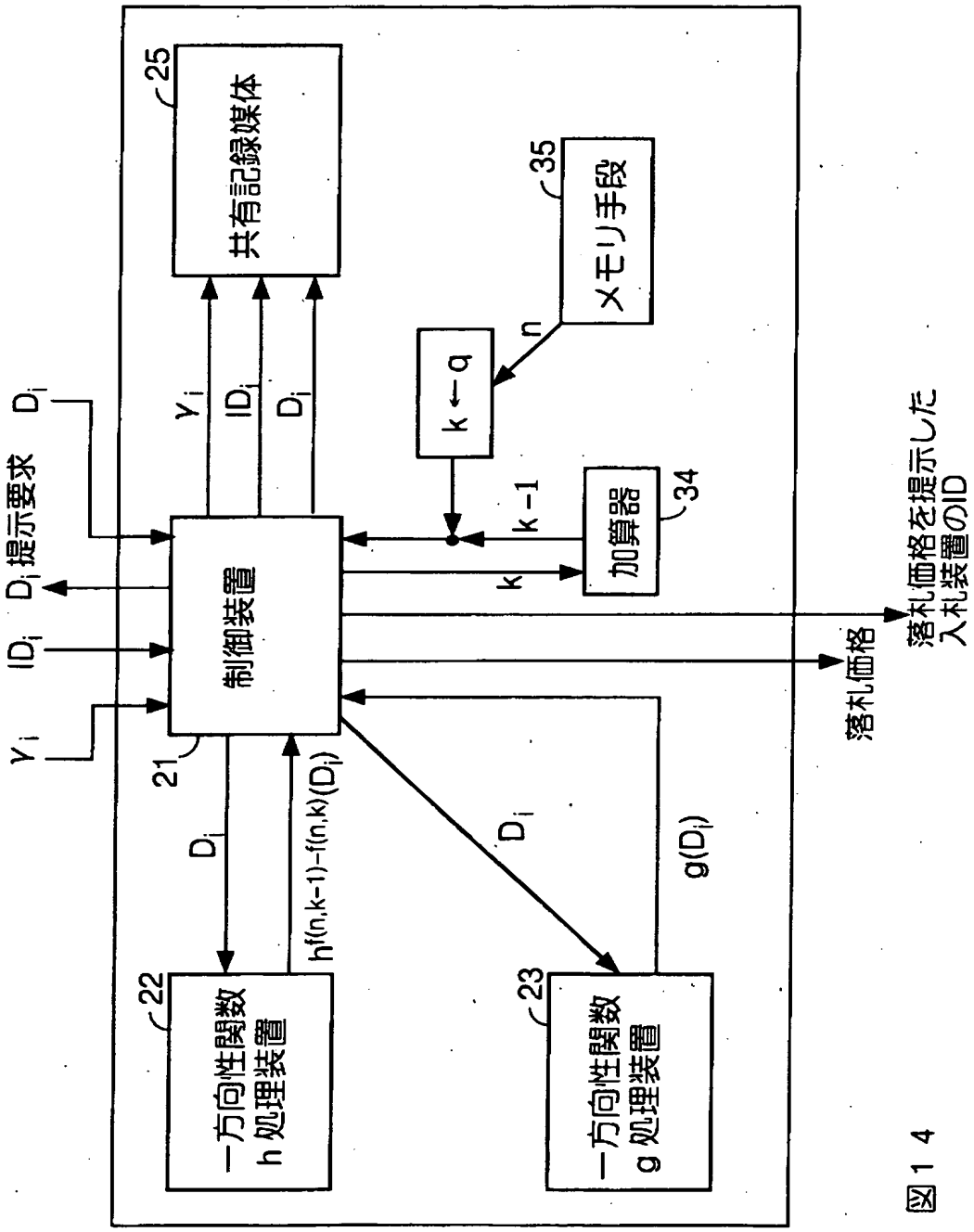
共有記録媒体
25
メモリ手段
35
n
k←q
加算器
34
k
k-1
制御装置
21
D_i
ID_i
γ_i
D_i 提示要求
落札価格
落札価格を提示した
入札装置のID
D_i
h^f(n,k-1)-f(n,k)(D_i)
D_i
g(D_i)
一方向性関数
h 処理装置
22
一方向性関数
g 処理装置
23

図１４

認定・付加情報

特許出願の番号	平成１１年　特許願　第２０５００４号
受付番号	５９９００７０２５６１
書類名	手続補正書
担当官	坏　政光　　８８４４
作成日	平成１１年　７月２７日

＜認定情報・付加情報＞

【補正をする者】

【識別番号】	000004226
【住所又は居所】	東京都千代田区大手町二丁目３番１号
【氏名又は名称】	日本電信電話株式会社

【代理人】　申請人

【識別番号】	100066153
【住所又は居所】	東京都新宿区新宿四丁目２番２１号　相模ビル
【氏名又は名称】	草野　卓

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　　東京都千代田区大手町二丁目３番１号
氏　名　　日本電信電話株式会社